



ARUBA WIRELESS AND CLEARPASS 6 INTEGRATION GUIDE



Technical Note

Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site::

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Audience	8
Typographic Conventions	8
Contacting Support	9
1. Aruba Wireless and ClearPass 6.0.1 Integration Guide	10
Purpose	10
Assumptions	10
Step 1: AOS Controller Configuration.....	10
Step 2: Adding a RFC 3576 Server	12
Step 3: Creating a new Server Group for ClearPass	14
Step 4: Create a Captive Portal role	20
Step 5: Pre-configured Firewall Policies.....	25
Step 6: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID.....	26
Step 7: Associating a 802.1x SSID and Guest SSID with AAA Profiles.....	32
Step 8: ClearPass Guest Setup	34
Basic Guest Registration and Login configuration	34
2. ClearPass Policy Manager Setup	39
Guest SSID Login service configuration	44
3. Testing the 802.1x and Guest SSID	48
Step 9: Test the 802.1x SSID	51
Step 10: Testing the Guest SSID	51
4. Testing the MAC Caching	54
5. Advanced Features	55
<i>Controller Management Login Authentication with ClearPass Policy Manager.....</i>	<i>55</i>
<i>RADIUS Enforcement (Generic) configuration.....</i>	<i>55</i>
6. Troubleshooting.....	62

Figure 1 Adding a RADIUS Server	11
Figure 2 RADIUS Server list.....	11
Figure 3 RADIUS server IP and Key entry	11
Figure 4 RFC 3576 Server list.....	12
Figure 5 Adding a RF 3576 Server.....	13
Figure 6 RFC 3576 Server IP	13
Figure 7 Enter the RADIUS shared key	14
Figure 8 ClearPass Server Group	14
Figure 9 Adding a ClearPass Server Group	15
Figure 10 ClearPass Server Group list	15
Figure 11 Adding a ClearPass RADIUS Server	16
Figure 12 Selecting the newly created ClearPass Server Group.....	16
Figure 13 Select Add Server ClearPass button	17
Figure 14 L3 Authentication tab.....	17
Figure 15 Select Captive Portal Authentication Profile.....	18
Figure 16 Enter a new Captive Portal profile name.....	18
Figure 17 Select the newly created Captive Portal Authentication Profile.....	19
Figure 18 Captive Portal Authentication Profile login page IP	19
Figure 19 Changing "default" server group to the newly created Captive Portal Authentication Profile server name...	20
Figure 20 The newly created Captive Portal Authentication Profile server Group	20
Figure 21 User Roles tab.....	21
Figure 22 Adding a User Role	21
Figure 23 Create new User Role Policy	22
Figure 24 Entering the Policy Name and Policy Type	22
Figure 25 Entering the ACL (Access Control List) field names	23
Figure 26 Firewall policy rule Add button.....	23
Figure 27 Adding a svc-https (tcp 443 Service ACL.....	24
Figure 28 Accepting the ACL rows created.....	24
Figure 29 User Roles Add page listings	24
Figure 30 Firewall logon-control (session) policy	25

Figure 31 Firewall “captiveportal (session)” policy	25
Figure 33 Firewall Policies list.....	26
Figure 33 Aruba_admin captive portal being chosen.....	26
Figure 34 Select the previously configured Captive Portal Profile	26
Figure 35 Adding a ClearPass Guest Profile	27
Figure 36 Changing the default Initial role	27
Figure 37 RADIUS Interim Accounting option	28
Figure 38 Log Accounting Interim-Update Packets option in CPPM.....	28
Figure 39 MAC Authentication Profile setting = default.....	29
Figure 40 MAC Authentication Server Group option	29
Figure 41 RADIUS Accounting Server Group option	30
Figure 42 RFC 3576 for this AAA Profile	31
Figure 43 IP address of your ClearPass server	31
Figure 44 Configuring no MAC Authentication Profile.....	32
Figure 45 Advanced Services All Profiles menu	32
Figure 46 Advanced Services Wireless LAN Profile.....	33
Figure 47 Advanced Services Virtual AP Profile.....	33
Figure 48 Virtual AP Profile modifications.....	34
Figure 49 Policy Manager login	34
Figure 50 ClearPass Policy Manager Dashboard.....	35
Figure 51 ClearPass Guest Quick Link	35
Figure 52 ClearPass Guest administration page.....	36
Figure 53 ClearPass Guest Self-Registration selection	36
Figure 54 ClearPass Guest Self-Registration menu	37
Figure 55 NAS Vendor Settings.....	37
Figure 56 Enable guest login to a Network Access Server	38
Figure 57 ClearPass Policy Manager Network Devices selection	39
Figure 58 Add a ClearPass Policy Manager Network Device	39
Figure 59 Configuring a ClearPass Policy Manager Network Device	40
Figure 60 Aruba 802.1X Wireless 'Start Here' selection.....	40
Figure 61 Naming a 802.1X Wireless Service	41
Figure 62 802.1X Authentication Methods and Sources.....	41
Figure 63 802.1X Role Mapping Policy	42
Figure 64 802.1X Enforcement configuration	42
Figure 65 ClearPass Policy Manager Reorder menu	43

Figure 66 Reorder Services 'Move Up' process.....	44
Figure 67 Guest Access With MAC Caching	44
Figure 68 Service Rule Guest SSID conditions.....	45
Figure 69 Service Rule Guest MAC Authentication conditions	45
Figure 70 Adding a Local User Repository Device.....	45
Figure 71 Adding a Identity Role	46
Figure 72 Guest SSID Local User conditions	47
Figure 73 Configuring Enforcement Profiles	48
Figure 74 Adding a new Enforcement Profile	49
Figure 75 Enforcement Profile Attributes.....	49
Figure 76 Enforcement Policies rule configuration	50
Figure 77 Enforcement Authenticated Profile Rules Editor.....	50
Figure 78 Live Monitoring Access Tracker menu	51
Figure 79 802.1x SSID RADIUS, ACCEPT WLAN Enterprise Service	51
Figure 80 MAC Auth REJECT for the MAC Caching on the Guest SSID	51
Figure 81 ClearPass Guest Login	52
Figure 82 ClearPass Guest Registration.....	52
Figure 83 ClearPass Guest Registration Receipt	52
Figure 84 RADIUS, ACCEPT configuration for a newly created 802.1x SSID Guest account.....	53
Figure 85 Successful MAC authentication	54
Figure 86 Adding a Controller Management Local User.....	55
Figure 87 RADIUS Enforcement (Generic) template	55
Figure 88 RADIUS Enforcement (Generic) Service Rules configuration.....	56
Figure 89 RADIUS Enforcement (Generic) Authentication configuration	56
Figure 90 RADIUS Enforcement (Generic) Enforcement configuration	57
Figure 91 RADIUS Enforcement (Generic) Enforcement Profile Template and Name.....	57
Figure 92 RADIUS Enforcement (Generic) Enforcement Attribute configuration	57
Figure 93 RADIUS Enforcement (Generic) Enforcement configuration Summary	58
Figure 94 RADIUS Enforcement (Generic) Rule Conditions and Enforcement Profiles	59
Figure 95 RADIUS Enforcement (Generic) Enforcement Rules Profile Summary.....	59
Figure 96 RADIUS Enforcement (Generic) Enforcement Policy Service Creation Flow	60

Audience

This Aruba Wireless and ClearPass 6 Integration Guide is intended for system administrators and people who are integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1.

Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts.

Type Style	Description
<i>Italics</i>	Used to emphasize important items and for the titles of books.
Boldface	Used to highlight navigation in procedures and to emphasize command names and parameter options when mentioned in text.
Sample template code or HTML text	Code samples are shown in a fixed-width font.
<angle brackets>	When used in examples or command syntax, text within angle brackets represents items you should replace with information appropriate to your specific situation. For example: <pre>ping <ipaddr></pre> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	https://licensing.arubanetworks.com/
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support-services/security-bulletins/

Support Email Addresses

Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email	wsirt@arubanetworks.com

Please email details of any security problem found in an Aruba product.



1. Aruba Wireless and ClearPass 6.0.1 Integration Guide

Purpose

The purpose of this document is to provide instructions for integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1. This will include basic topics for 802.1x, RADIUS, and Guest integration in an environment using an Aruba Networks WLAN Solution.

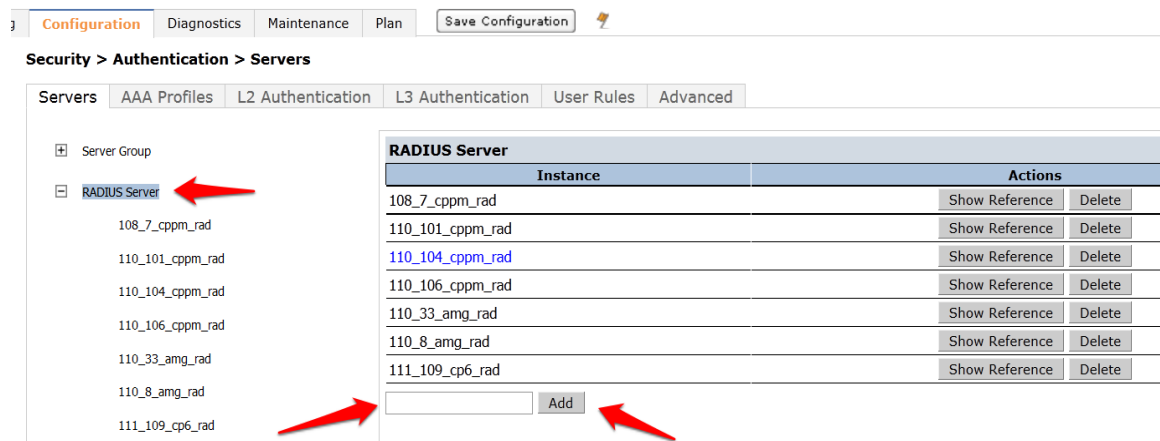
Assumptions

1. Aruba Networks wireless controller is setup and running the latest code.
2. At least one access point is provisioned on the controller for testing.
3. 802.1x SSID is already configured.
4. Guest SSID with Captive Portal is already configured.
5. DHCP and DNS are appropriately configured.
6. ClearPass 6.0.1 server (VM or Physical Appliance) initial setup is complete. This includes network settings, time and date, and system name.
7. Aruba Wireless controller can communicate with ClearPass 6.0.1.
8. The Guest SSID VLAN can communicate with ClearPass 6.0.1.
9. All systems are appropriately licensed.
10. Only one interface is configured on ClearPass.

Step 1: AOS Controller Configuration

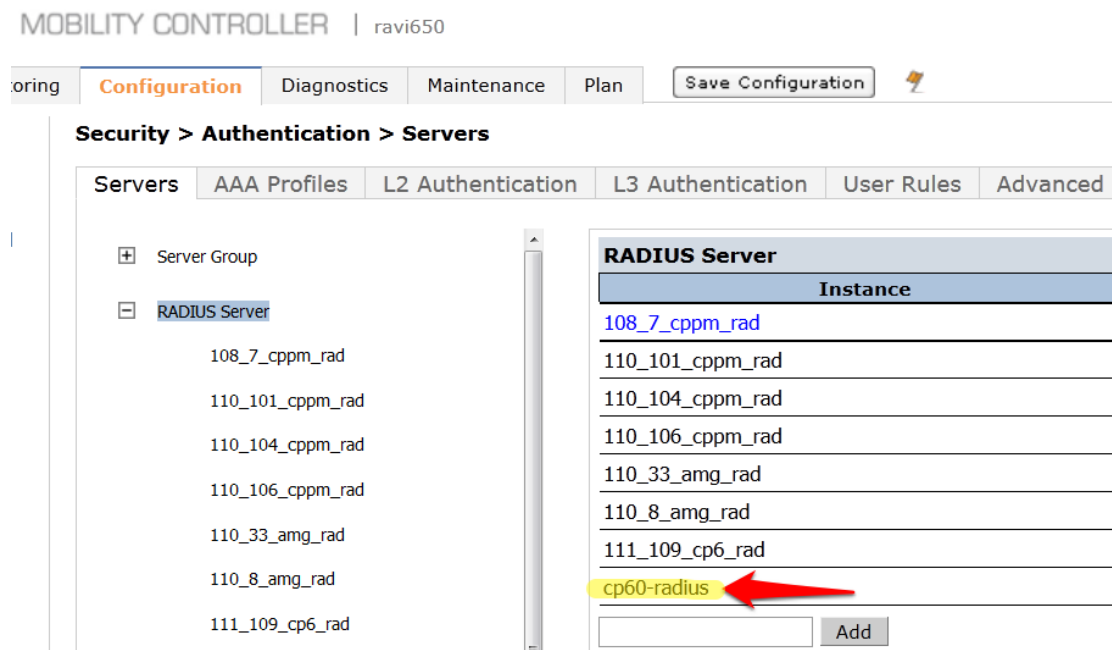
Login to the controller GUI as an admin user. Navigate to **Configuration->Security->Authentication->Servers** tab. Click on **RADIUS Server** and create a new RADIUS server by entering the new RADIUS server reference name in the empty Add box and clicking **Add**.

Figure 1 Adding a RADIUS Server



Click on the new server name that shows up in the RADIUS Server list on that page:

Figure 2 RADIUS Server list



Enter the IP address for ClearPass in the **Host** field. Enter <aruba123> for the **key**. Click **Apply** at the bottom of the page to save these configuration settings.

Figure 3 RADIUS server IP and Key entry

RADIUS Server > cp60-radius Show Reference Save As Reset

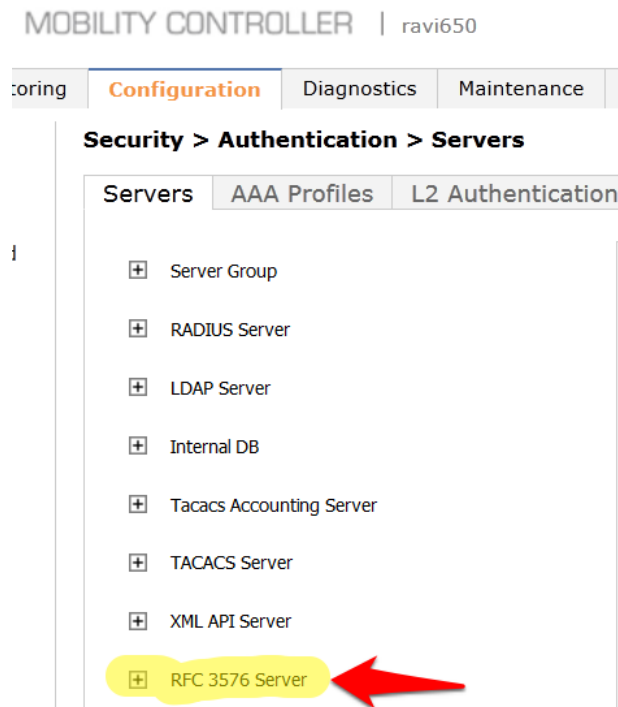
Host	10.1.1.20	Key	 Retype:
Auth Port	1812	Acct Port	1813
Retransmits	3	Timeout	5 sec
NAS ID		NAS IP	
Source Interface		Use MD5	☐
Use IP address for calling station ID	☐	Mode	☒

Step 2: Adding a RFC 3576 Server

The next step is to add an RFC 3576 server entry for ClearPass.

Click on **RFC 3576 Server**.

Figure 4 RFC 3576 Server list



Enter the **IP address** of ClearPass in the entry box and click **Add**.

Figure 5 Adding a RF 3576 Server

MOBILITY CONTROLLER | ravi650

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > Servers

Servers	AAA Profiles	L2 Authentication	L3 Authentication	User Rules				
+ Server Group + RADIUS Server + LDAP Server + Internal DB + Tacacs Accounting Server + TACACS Server + XML API Server - RFC 3576 Server					RFC 3576 Server Instance 10.162.108.7 10.162.108.9 10.162.110.19 10.162.110.24 10.162.110.25 10.162.110.26 10.162.110.33 10.162.110.36 10.162.110.37 10.162.110.8 10.162.111.109 10.2.50.178 10.6.52.81 10.1.1.20 Add			

Click on the IP address of ClearPass that appears in the left column under RFC 3576 Server.

Figure 6 RFC 3576 Server IP

MOBILITY CONTROLLER | ravi650

Configuration | Diagnostics | Maintenance

Security > Authentication > Servers

Servers	AAA Profiles	L2 Authentication
+ Server Group + RADIUS Server + LDAP Server + Internal DB + Tacacs Accounting Server + TACACS Server + XML API Server - RFC 3576 Server		

10.1.1.20

You will be presented with a screen in the right column that looks like this:

Figure 7 Enter the RADIUS shared key

RFC 3576 Server > 10.1.1.20 Show Reference Save As Reset

Key	
	Retype:

1. You **MUST** enter the RADIUS shared key into the key boxes. Enter <aruba123> in both boxes and click **Apply** at the bottom of the page to save the changes.

Note: This step is extremely important!

Step 3: Creating a new Server Group for ClearPass

The next step is to create a new Server Group for ClearPass. Click on Server Group.

Figure 8 ClearPass Server Group

MOBILITY CONTROLLER | ravi650

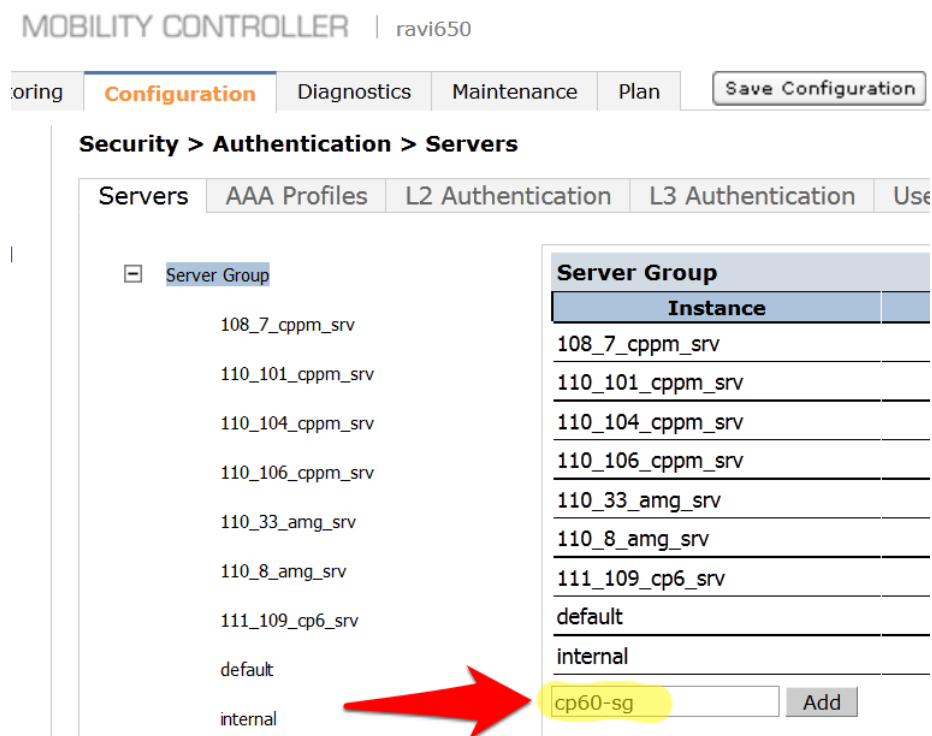
oring **Configuration** Diagnostics Maintenance Plan

Security > Authentication > Servers

Servers	AAA Profiles	L2 Authentication	L3 /
☐ Server Group			
☐ RADIUS Server			
☐ LDAP Server			
☐ Internal DB			
☐ Tacacs Accounting Server			
☐ TACACS Server			
☐ XML API Server			
☐ RFC 3576 Server			
☐ Windows Server			

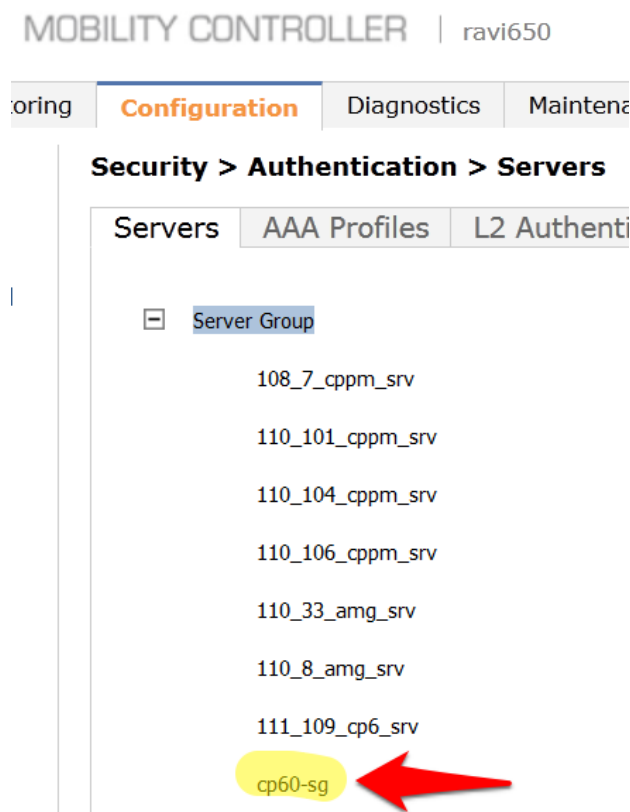
Enter a reference name for your ClearPass Server Group in the empty box and click **Add**.

Figure 9 Adding a ClearPass Server Group



Select the newly created Server Group on the right under Server Group:

Figure 10 ClearPass Server Group list

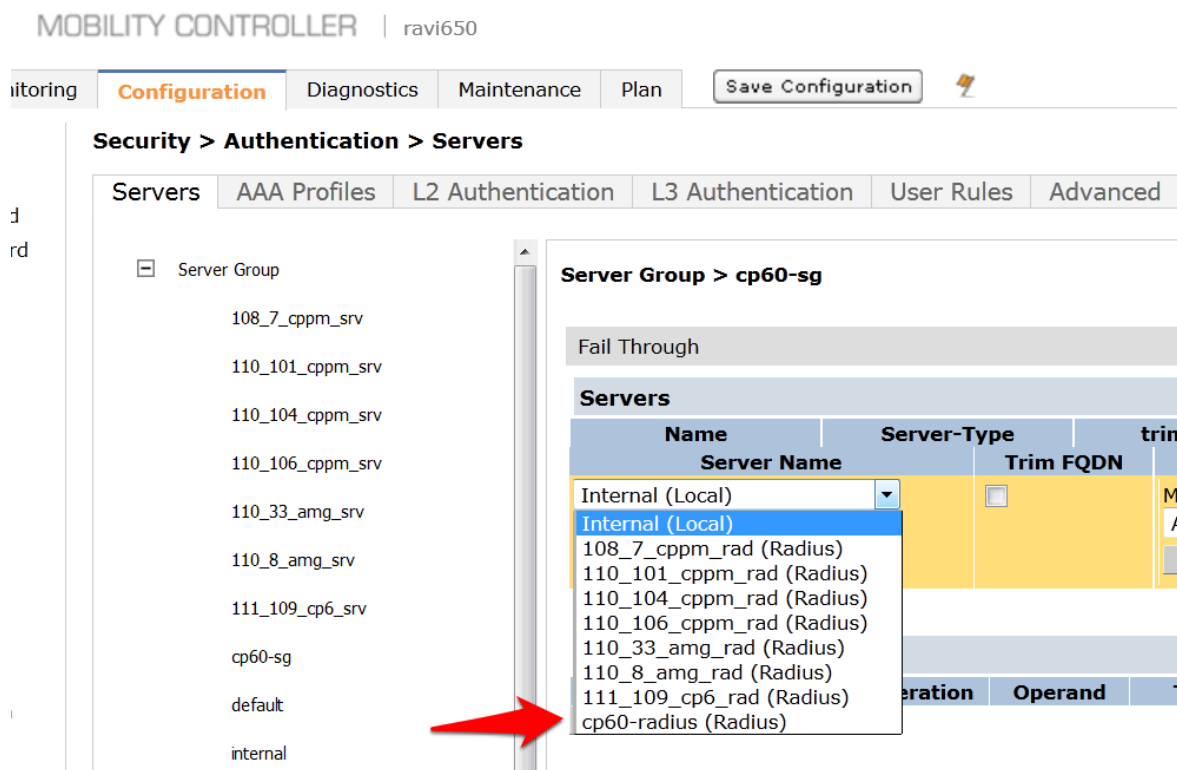


Click **New** and select the ClearPass RADIUS server from the previous step.

Figure 11 Adding a ClearPass RADIUS Server



Figure 12 Selecting the newly created ClearPass Server Group



2. Click **Add Server**. Click **Apply** at the bottom of the page to save the changes.

Figure 13 Select Add Server ClearPass button

Server Group > cp60-sg Show Reference Save As Reset

Fail Through ☐

Servers

Name	Server-Type	trim-FQDN	Match-Rule	Actions
Server Name	Trim FQDN	Match Type	Operator	Match String
cp60-radius (Radius)	☐	Authstring	contains	
		Add Rule	Delete Rule	

Add Server Cancel

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated	Actions
New								

Captive Portal profile

Click on the **L3 Authentication** tab.

Figure 14 L3 Authentication tab

MOBILITY CONTROLLER | ravi650

oring **Configuration** Diagnostics Maintenance Plan Save Configuration

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication **L3 Authentication** User Rule

☐ Server Group

- 108_7_cppm_srv
- 110_101_cppm_srv
- 110_104_cppm_srv
- 110_106_cppm_srv
- 110_33_amg_srv
- 110_8_amg_srv
- 111_109_cp6_srv
- cp60-sg**
- default
- internal

Server Group > cp60-sg

Fail Through

Servers

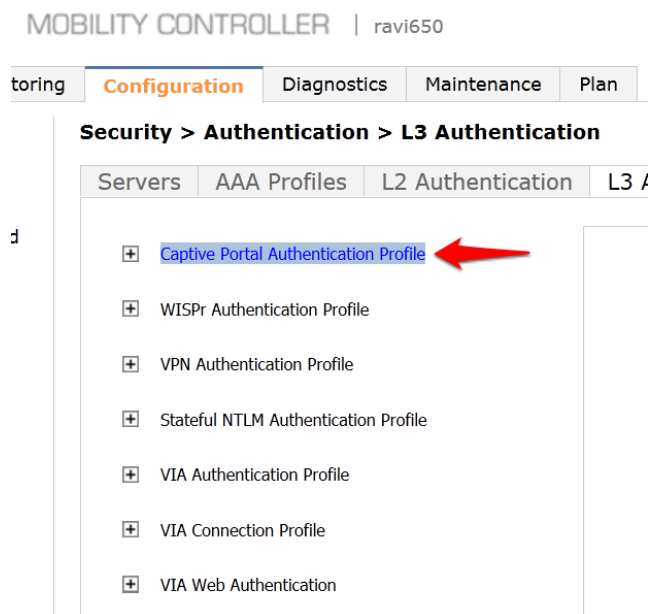
Name	Server-Type
Server Name	
cp60-radius (Radius)	

Server Rules

Priority	Attribute	Operation
New		

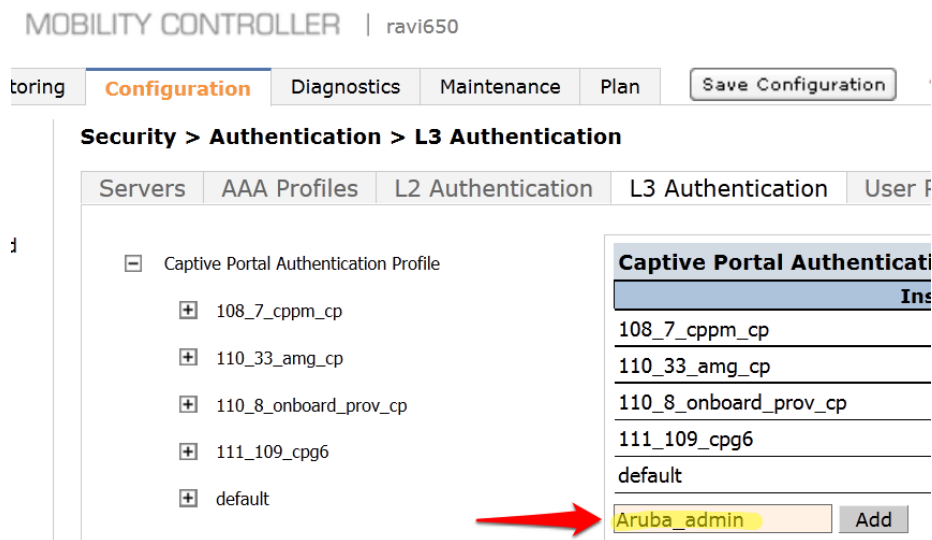
Click on **Captive Portal Authentication Profile**.

Figure 15 Select Captive Portal Authentication Profile



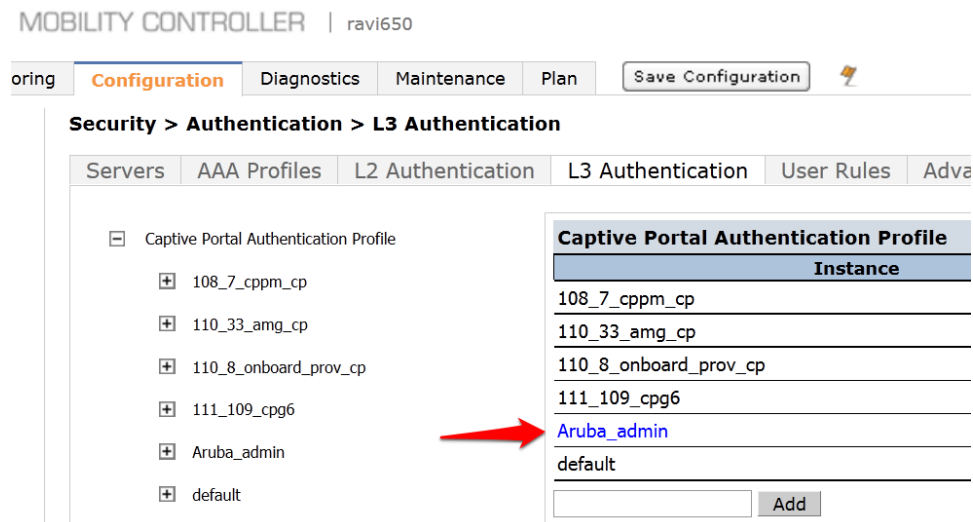
Enter a new Captive Portal profile name in the empty box and click **Add**.

Figure 16 Enter a new Captive Portal profile name



Select the newly created **Captive Portal Authentication Profile** under **Captive Portal Authentication Profile** on the right.

Figure 17 Select the newly created Captive Portal Authentication Profile



There are two things we need to change on this profile.

3. Change the **Login page** to http://10.1.1.20/guest/guest_register_login.php (replacing the 10.1.1.20 with the IP address of your ClearPass 6.0.1 server).

Figure 18 Captive Portal Authentication Profile login page IP

Captive Portal Authentication Profile > Aruba_admin Show Reference Save As Reset

Default Role	guest	Default Guest Role	guest
Redirect Pause	10 sec	User Login	☒
Guest Login	☐	Logout popup window	☒
Use HTTP for authentication	☐	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	☐
Use CHAP (non-standard)	☐	Login page	10.162.111.119
Welcome page	/auth/welcome.html	Show Welcome Page	☒
Add switch IP address in the redirection URL	☐	Adding user vlan in redirection URL	☐
Add a controller interface in the redirection URL		Allow only one active user session	☐
White List	Delete Add	Black List	Delete Add
Show the acceptable use policy page	☐		

Click **Apply** at the bottom to save the changes.

4. Click on **Server Group** under the **Captive Portal Authentication Profile** and change the **Server Group** from **default** to the Server Group that you created for ClearPass in the previous steps and click **Apply** at the bottom of the page to save the changes.

Figure 19 Changing "default" server group to the newly created Captive Portal Authentication Profile server name

Security > Authentication > L3 Authentication

The screenshot shows the 'L3 Authentication' tab in the configuration interface. On the left, under 'Captive Portal Authentication Profile', there is a list of server groups. The 'default' server group is highlighted. On the right, the 'Server Group' dropdown menu is open, showing a list of server groups. The 'cp60-sg' option is highlighted with a red arrow, indicating it is the selected group to be applied to the 'default' server group.

Figure 20 The newly created Captive Portal Authentication Profile server Group

Security > Authentication > L3 Authentication

The screenshot shows the 'L3 Authentication' tab in the configuration interface. On the left, under 'Captive Portal Authentication Profile', there is a list of server groups. The 'cp60-sg' server group is highlighted with a red arrow. On the right, the 'Server Group' dropdown menu is open, showing a list of server groups. The 'cp60-sg' option is highlighted with a red arrow, indicating it is the selected group to be applied to the 'default' server group.

Step 4: Create a Captive Portal role

Now we need to create our Captive Portal role, which is the role that clients will receive when they connect to the Guest SSID.

Navigate to **Configuration->Security->Access Control->User Roles** tab. Click **Add** to create a new User Role.

Figure 21 User Roles tab

Security > Access Control > User Roles

User Roles	System Roles	Policies	Time Ranges	Guest Access
Name	Firewall Policies	Bandwidth Contract	Actions	
108_7_cppm_cp	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
110_33_amg_logon	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
110_8_onboard_prov_logon	110_8_onboard_prov_cp_list_operations/,logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
111_109_cpg6_logon	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
authenticated	allowall/,v6-allowall/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
default-via-role	allowall/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
default-vpn-role	allowall/,v6-allowall/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
denyall	Not Configured	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
guest	http-acl/,https-acl/,dhcp-acl/,icmp-acl/,dns-acl/,v6-http-acl/,v6-https-acl/,v6-dhcp-acl/,v6-icmp-acl/,v6-dns-acl/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
guest-logon	v6-logon-control/,captiveportal6/,logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
logon	ocsp-acl/,captiveportal6/,logon-control/,captiveportal/,vpnlogon/,v6-logon-control/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
voice	sip-acl/,noe-acl/,svp-acl/,vocera-acl/,skinny-acl/,h323-acl/,dhcp-acl/,tftp-acl/,dns-acl/,icmp-acl/	Up:Not Enforced Down:Not Enforced	Show Reference	Edit Delete
Add				

Enter a name like <CPG-Login> for the **Role Name** under **Firewall Policies**, Click **Add**.

Figure 22 Adding a User Role

Security > User Roles > Add Role

User Roles	System Roles	Policies	Time Ranges	Guest Access
------------	--------------	----------	-------------	--------------

Role Name

CPG-Login

Firewall Policies

Name	Rule Count
Add	

For the first policy, it is essentially important that we add an ACL that will allow our **Guest user** to access ClearPass 6.0.1, which is where the Captive Portal webpage will be hosted.

Choose the radio button for **Create New Policy**, and click the **Create** button:

Figure 23 Create new User Role Policy

Security > User Roles > Add Role

User Roles | System Roles | Policies | Time Ranges | Guest Access

Role Name

Firewall Policies

Name	Rule Count
Add	
☐ Choose From Configured Policies	validuser (session)
☐ Create New Policy From Existing Policy	validuser (session)
☒ Create New Policy	Create

Enter and select the following information:

- **Policy Name:** <CP6-web-ACL>
- **Policy Type:** <Session>

Click **Add**.

Figure 24 Entering the Policy Name and Policy Type

Security > User Roles > Add Role > Add New Policy

User Roles | System Roles | Policies | Time Ranges | Guest Access

Policy Name

Policy Type

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time
Add								

Select and enter the following information for the first line of the ACL:

- **IP Version:** <IPv4>
- **Source:** <User>
- **Destination:** host
 - **Host IP:** (the IP address of your ClearPass server)
- **Service:** <service>
 - **Service:** <svc-http (tcp 80)>

- **Action:** <permit>

Figure 25 Entering the ACL (Access Control List) field names

Security > User Roles > Add Role > Add New Policy

Policy Name: CP6-web-ACL

Policy Type: Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time
IPv4	user	host Host IP 10.162.111.119	service Service svc-http (tcp 80) New	permit				

Click **Add** at the far right underneath this rule.

Figure 26 Firewall policy rule Add button

« Back

Classify Media	TOS	802.1p Priority	Action
☐			

Add Cancel

Done

Click **Add** again to add another line to this ACL, identical to the previous line except:

Choose **Service: svc-https (tcp 443)**

Figure 27 Adding a svc-https (tcp 443 Service ACL

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name CP6-web-ACL

Policy Type Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time R
IPv4	user	host 10.162.111.119	svc-http	permit			low	

Add

IP Version Source Destination Service Action

IPv4 user host Host IP 10.162.111.119 svc-https (tcp 443) permit

New

Click **Add** at the far right underneath this rule.

Figure 28 Accepting the ACL rows created

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name CP6-web-ACL

Policy Type Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue
IPv4	user	host 10.162.111.119	svc-http	permit			low
IPv4	user	host 10.162.111.119	svc-https	permit			low

Add

Click **Done**

You will be brought back to the Add Role page where you were creating your CPG-Login User Role.

Figure 29 User Roles Add page listings

Security > User Roles > Add Role

User Roles System Roles Policies Time Ranges Guest Access

Role Name CPG-login

Firewall Policies

Name	Rule Count
CP6-web-ACL	2

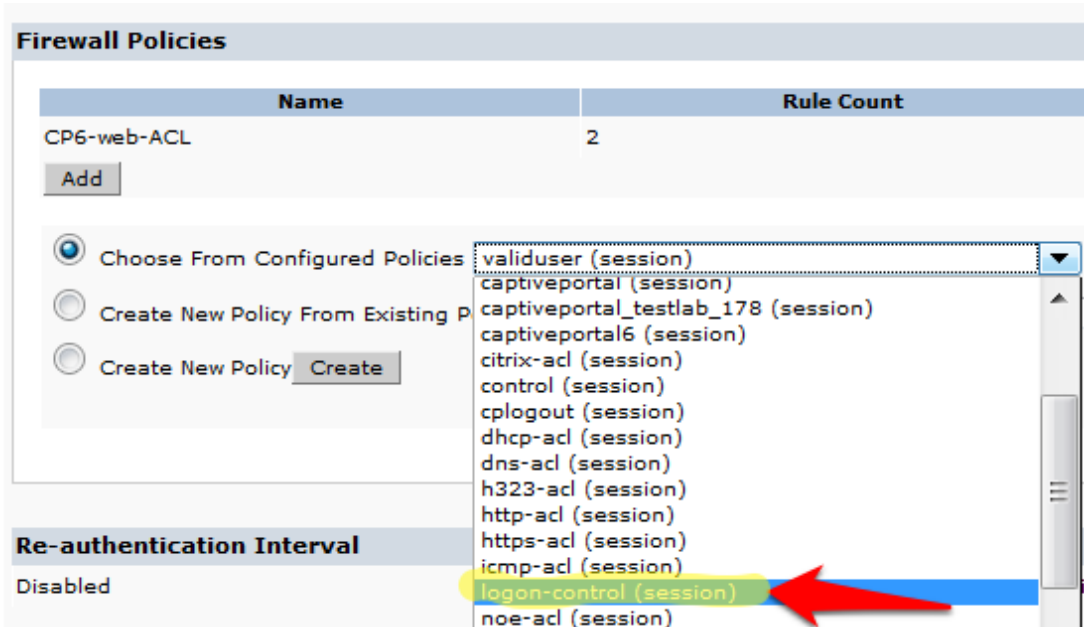
Add

Step 5: Pre-configured Firewall Policies

The Firewall Policy that you just created has been added to the list. Now we need to add two more pre-configured Firewall Policies.

Click **Add** under **Firewall Policies**. Select the radio button for **Choose From Configured Policies** and select the policy called **logon-control (session)**.

Figure 30 Firewall logon-control (session) policy

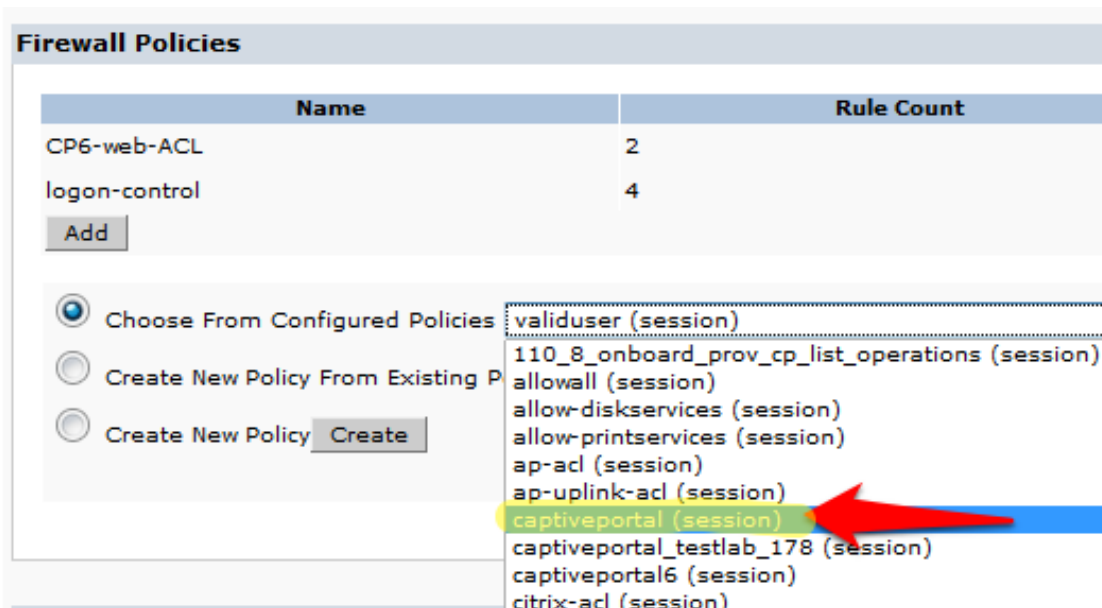


Click **Done** in the **Firewall Policies** section.

Click **Add** again in the **Firewall Policies** section.

Select the radio button for **Choose From Configured Policies** and select the policy called **captiveportal (session)**.

Figure 31 Firewall "captiveportal (session)" policy



Click **Done** in the **Firewall Policies** section. Your Firewall Policy should look like this:

Figure 32 Firewall Policies list

Firewall Policies		
Name	Rule Count	Location
CP6-web-ACL	2	
logon-control	4	
captiveportal	8	
Add		

NOTE: The Firewall policy order **MUST** place “captive portal” at the **bottom** of the list!

Scroll down this page to the **Captive Portal Profile** section.

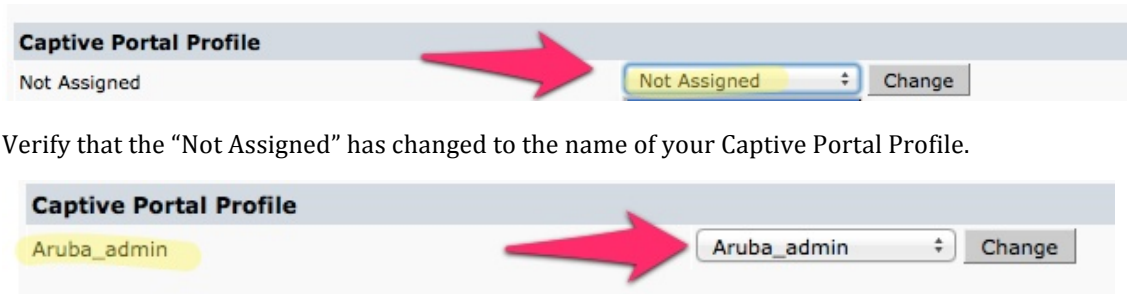
Select the previously configured Captive Portal Profile from the drop-down list.

Figure 33 Aruba_admin captive portal being chosen



Click the **Change** button.

Figure 34 Select the previously configured Captive Portal Profile



Click **Apply** at the bottom of the page to save the newly created User Role.

Step 6: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID

The next step is to create AAA Profiles for the ClearPass Guest and 802.1x SSID.

Navigate to **Configuration->Security->Authentication->AAA Profiles** tab.

Click **Add**, enter a name for the ClearPass Guest Profile, and then click **Add** again.

Figure 35 Adding a ClearPass Guest Profile

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > Profiles

Servers | **AAA Profiles** | L2 Authentication | L3 Authentication | User Rules | Advanced

AAA Profile

- 108_7_cppm_health
- 108_7_onboard_1ssid
- 108_7_onboard_dot1x_aaa
- 110_101_cppm_dot1x_aaa
- 110_104_cppm_dot1x_aaa
- 110_106_cppm_dot1x_aaa
- 110_33_amg_aaa
- 110_8_onboard_dot1x_aaa
- 110_8_onboard_prov_aaa
- 111_109_cpg_aaa
- default
- default-dot1x
- default-dot1x-psk
- default-mac-auth
- default-open
- default-xml-api
- NoAuthAAAProfile

AAA Profiles Summary

Name	
108_7_cppm_health	108_7_cpp
108_7_onboard_1ssid	logon
108_7_onboard_dot1x_aaa	logon
110_101_cppm_dot1x_aaa	logon
110_104_cppm_dot1x_aaa	logon
110_106_cppm_dot1x_aaa	logon
110_33_amg_aaa	110_33_ar
110_8_onboard_dot1x_aaa	logon
110_8_onboard_prov_aaa	110_8_ont
111_109_cpg_aaa	111_109_c
default	guest-logo
default-dot1x	logon
default-dot1x-psk	guest-logo
default-mac-auth	logon
default-open	logon
default-xml-api	logon
NoAuthAAAProfile	logon

Add

Now in the left column, click on the new profile that you just created. Change the Initial role to the role that you created in Step 4: Create a Captive Portal role page 20.

Figure 36 Changing the default Initial role

AAA Profile > cp-60_cpg

Initial role	CPG-Login
802.1X Authentication Default Role	BYOD-Provision
RADIUS Interim Accounting	CPG-Login
Wired to Wireless Roaming	ap-role
Device Type Classification	authenticated
	cpbase
	cpguest-logon
	default-via-role
	default-vpn-role
	default

Tech Tip: On this page you will see an option for **RADIUS Interim Accounting**. This should be checked if you want live utilization updates in ClearPass, usually used to control guest users based on Bandwidth Utilization.

Figure 37 RADIUS Interim Accounting option

Security > Authentication > Profiles

Servers	AAA Profiles	L2 Authentication	L3 Authentication	User Rules	Advanced										
AAA Profile 108_7_cpmm_health 108_7_onboard_1ssid 108_7_onboard_dot1x_aaa 110_101_cpmm_dot1x_aaa 110_104_cpmm_dot1x_aaa 110_106_cpmm_dot1x_aaa AAA Profile > cp-60_cpg <table border="1"> <tr> <td>Initial role</td> <td>108_7_cpmm_cp</td> </tr> <tr> <td>802.1X Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>RADIUS Interim Accounting</td> <td>☒</td> </tr> <tr> <td>Wired to Wireless Roaming</td> <td>☒</td> </tr> <tr> <td>Device Type Classification</td> <td>☒</td> </tr> </table>						Initial role	108_7_cpmm_cp	802.1X Authentication Default Role	guest	RADIUS Interim Accounting	☒	Wired to Wireless Roaming	☒	Device Type Classification	☒
Initial role	108_7_cpmm_cp														
802.1X Authentication Default Role	guest														
RADIUS Interim Accounting	☒														
Wired to Wireless Roaming	☒														
Device Type Classification	☒														

Note: This also needs to be enabled on ClearPass.

In ClearPass Policy Manager, navigate to:

Administration->Server Manager->Server Configuration->Select Server->Service Parameters->RADIUS Server->Log Accounting Interim-Update Packets="TRUE".

Figure 38 Log Accounting Interim-Update Packets option in CPPM

ARUBA networks

Dashboard

Monitoring

Configuration

Administration

Users and Privileges

Server Manager

Server Configuration

Log Configuration

Local Shared Folders

Licensing

External Servers

Certificates

Dictionaries

Agents and Software Updates

ClearPass Policy Manager

Administration » Server Manager » Server Configuration - burns.corp.airwave.com

Server Configuration - burns.corp.airwave.com (10.162.111.119)

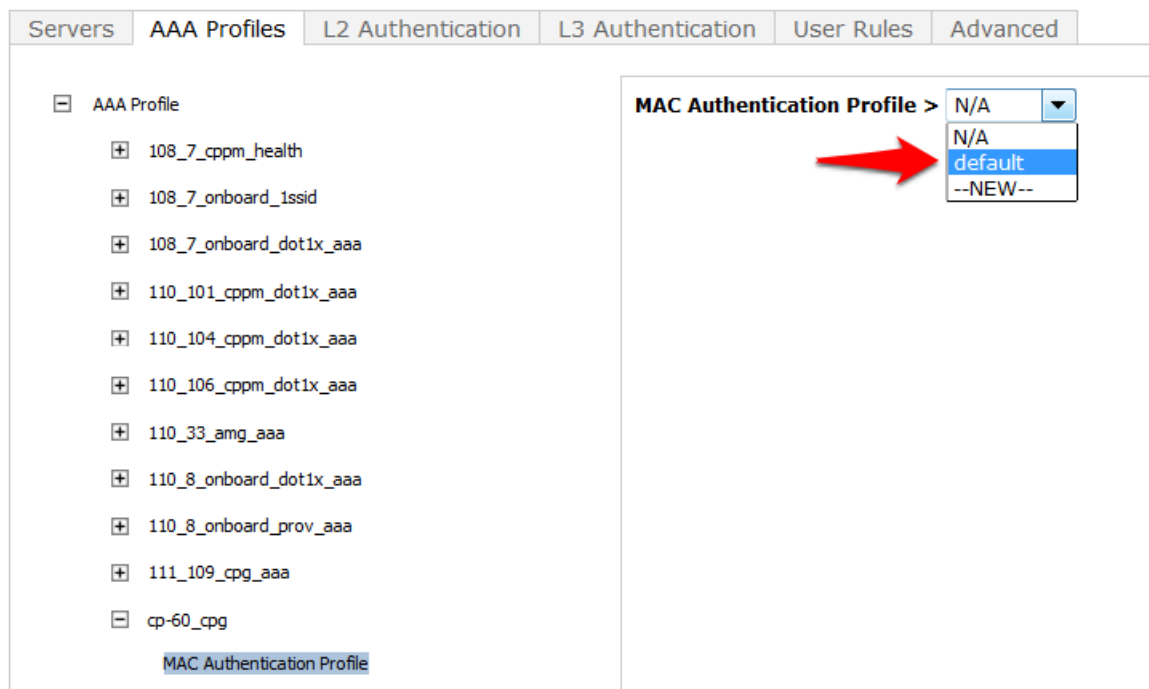
System	Services Control	Service Parameters	System Monitoring	Network Int
Cleanup Time		5	s	
Local DB Authentication Source Connection Count		32		
AD/LDAP Authentication Source Connection Count		64		
SQL DB Authentication Source Connection Count		32		
EAP-TLS Fragment Size		1024	b	
Use Inner Identity in Access-Accept Reply		FALSE		
Reject if OSCP response does not have Nonce		TRUE		
TLS Session Cache Limit		3750	s	
Thread Pool				
Maximum Number of Threads		10	tl	
Number of Initial Threads		5	tl	
EAP-FAST				
Master Key Expire Time		1	weeks	
Master Key Grace Time		3	weeks	
PACs are valid across cluster		true		
Accounting				
Log Accounting Interim-Update Packets		FALSE		
Back to Server Configuration				

Set the subsections of the profile as described below, clicking **Apply** after each change:

MAC Authentication Profile: default

Figure 39 MAC Authentication Profile setting = default

Security > Authentication > Profiles

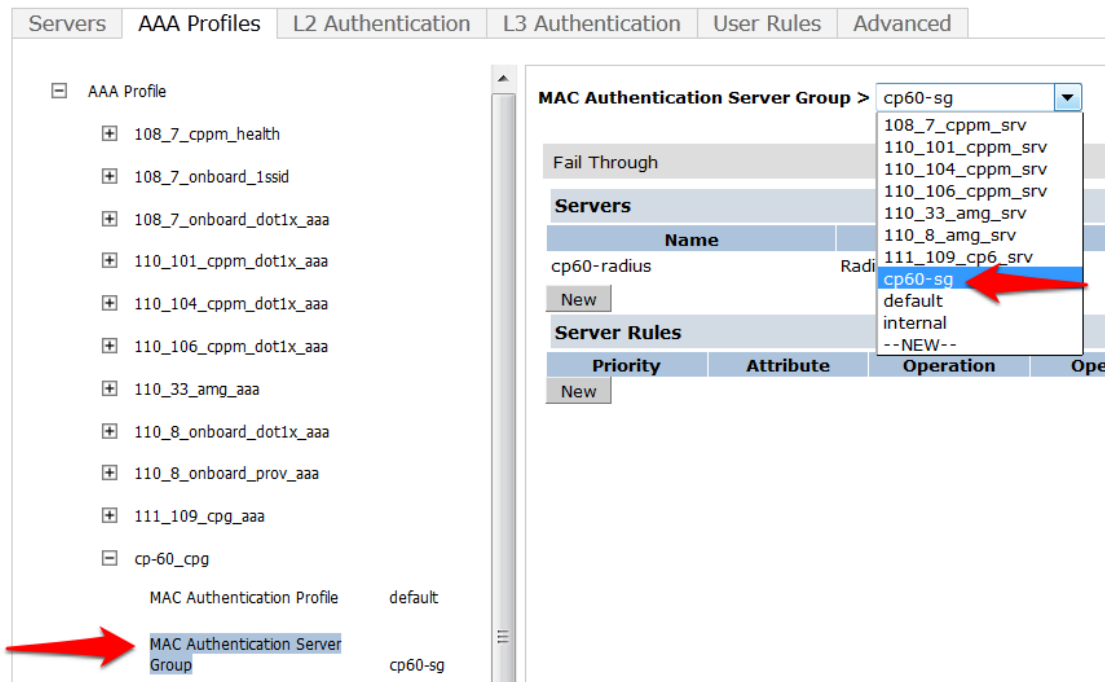


The screenshot shows the 'Security > Authentication > Profiles' configuration page. On the left, under 'AAA Profile', there is a list of profiles including '108_7_cppm_health', '108_7_onboard_1ssid', '108_7_onboard_dot1x_aaa', '110_101_cppm_dot1x_aaa', '110_104_cppm_dot1x_aaa', '110_106_cppm_dot1x_aaa', '110_33_amg_aaa', '110_8_onboard_dot1x_aaa', '110_8_onboard_prov_aaa', '111_109_cpg_aaa', and 'cp-60_cpg'. Below this list is a 'MAC Authentication Profile' section. On the right, the 'MAC Authentication Profile' dropdown menu is open, showing 'N/A', 'default', and '--NEW--' options. A red arrow points to the 'default' option.

MAC Authentication Server Group: (Your ClearPass 6.0.1 Server Group)

Figure 40 MAC Authentication Server Group option

Security > Authentication > Profiles



The screenshot shows the 'Security > Authentication > Profiles' configuration page. On the left, under 'AAA Profile', there is a list of profiles including '108_7_cppm_health', '108_7_onboard_1ssid', '108_7_onboard_dot1x_aaa', '110_101_cppm_dot1x_aaa', '110_104_cppm_dot1x_aaa', '110_106_cppm_dot1x_aaa', '110_33_amg_aaa', '110_8_onboard_dot1x_aaa', '110_8_onboard_prov_aaa', '111_109_cpg_aaa', and 'cp-60_cpg'. Below this list is a 'MAC Authentication Profile' section. On the right, the 'MAC Authentication Server Group' dropdown menu is open, showing 'cp60-sg', '108_7_cppm_srv', '110_101_cppm_srv', '110_104_cppm_srv', '110_106_cppm_srv', '110_33_amg_srv', '110_8_amg_srv', '111_109_cp6_srv', 'cp60-sg', 'default', 'internal', and '--NEW--' options. A red arrow points to the 'cp60-sg' option. In the bottom left, a red arrow points to the 'MAC Authentication Server Group' label.

RADIUS Accounting Server Group: (Your ClearPass 6.0.1 Server Group)

Figure 41 RADIUS Accounting Server Group option

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile

108_7_cppm_health

108_7_onboard_1ssid

108_7_onboard_dot1x_aaa

110_101_cppm_dot1x_aaa

110_104_cppm_dot1x_aaa

110_106_cppm_dot1x_aaa

110_33_amg_aaa

110_8_onboard_dot1x_aaa

110_8_onboard_prov_aaa

111_109_cpg_aaa

cp-60_cpg

MAC Authentication Profile default

MAC Authentication Server Group cp60-sg

802.1X Authentication Profile

802.1X Authentication Server Group

RADIUS Accounting Server Group cp60-sg

RADIUS Accounting Server Group >

cp60-sg

N/A

108_7_cppm_srv

110_101_cppm_srv

110_104_cppm_srv

110_106_cppm_srv

110_33_amg_srv

110_8_amg_srv

111_109_cp6_srv

cp60-sg

default

internal

--NEW--

Fail Through

Servers

Name

cp60-radius

New

Server Rules

Priority

Attribute

New

Click on **RFC 3576** for this AAA Profile.

30 |

Aruba Wireless and ClearPass 6 | Integration Guide

Figure 42 RFC 3576 for this AAA Profile

Security > Authentication > Profiles

AAA Profile

- + 108_7_cppm_health
- + 108_7_onboard_1ssid
- + 108_7_onboard_dot1x_aaa
- + 110_101_cppm_dot1x_aaa
- + 110_104_cppm_dot1x_aaa
- + 110_106_cppm_dot1x_aaa
- + 110_33_amg_aaa
- + 110_8_onboard_dot1x_aaa
- + 110_8_onboard_prov_aaa
- + 111_109_cpg_aaa
- cp-60_cpg
 - MAC Authentication Profile
 - MAC Authentication Server Group default
 - 802.1X Authentication Profile
 - 802.1X Authentication Server Group
 - RADIUS Accounting Server Group
- + XML API server
- RFC 3576 server 
- + 10.162.111.119

From the **Add a profile** list, select the IP address of your ClearPass server and click the **Add** button.

Figure 43 IP address of your ClearPass server

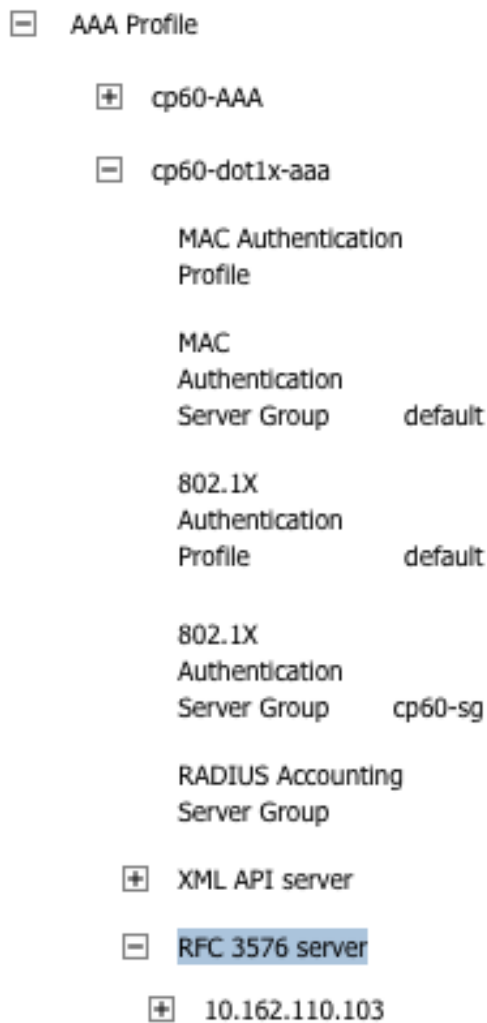
RFC 3576 servers
Name
10.162.111.119 

Add a profile: 10.1.1.20  Add

Click **Apply** to save these settings.

Repeat Creating AAA Profiles for the ClearPass Guest and 802.1x SSID, page 26, to create the AAA Profile for the 802.1x SSID. The only difference is that this AAA Profile will have 802.1x settings but no MAC Authentication Profile. See example below:

Figure 44 Configuring no MAC Authentication Profile



Step 7: Associating a 802.1x SSID and Guest SSID with AAA Profiles

The next step is to associate our 802.1x SSID and Guest SSID with the AAA Profiles we just created.

Navigate to **Configuration->Advanced Services->All Profiles**.

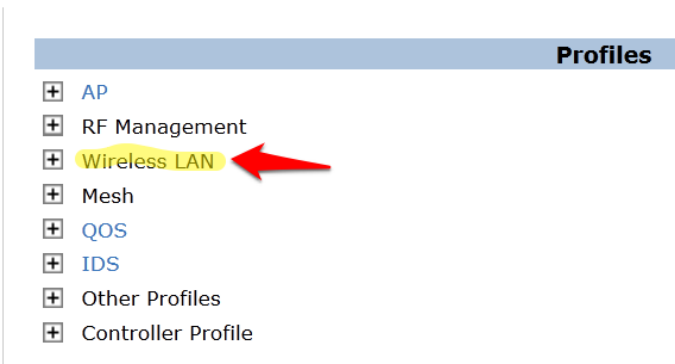
Figure 45 Advanced Services All Profiles menu



Expand the **Wireless LAN** section.

Figure 46 Advanced Services Wireless LAN Profile

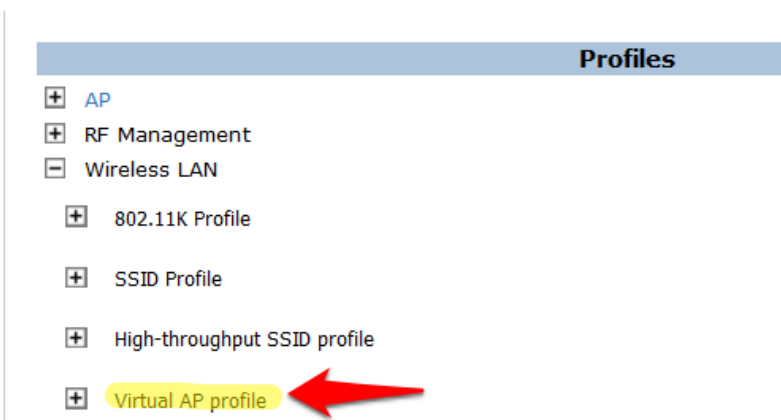
Advanced Services > All Profile Management



Expand the **Virtual AP profile** and locate your Guest and 802.1x SSID profiles.

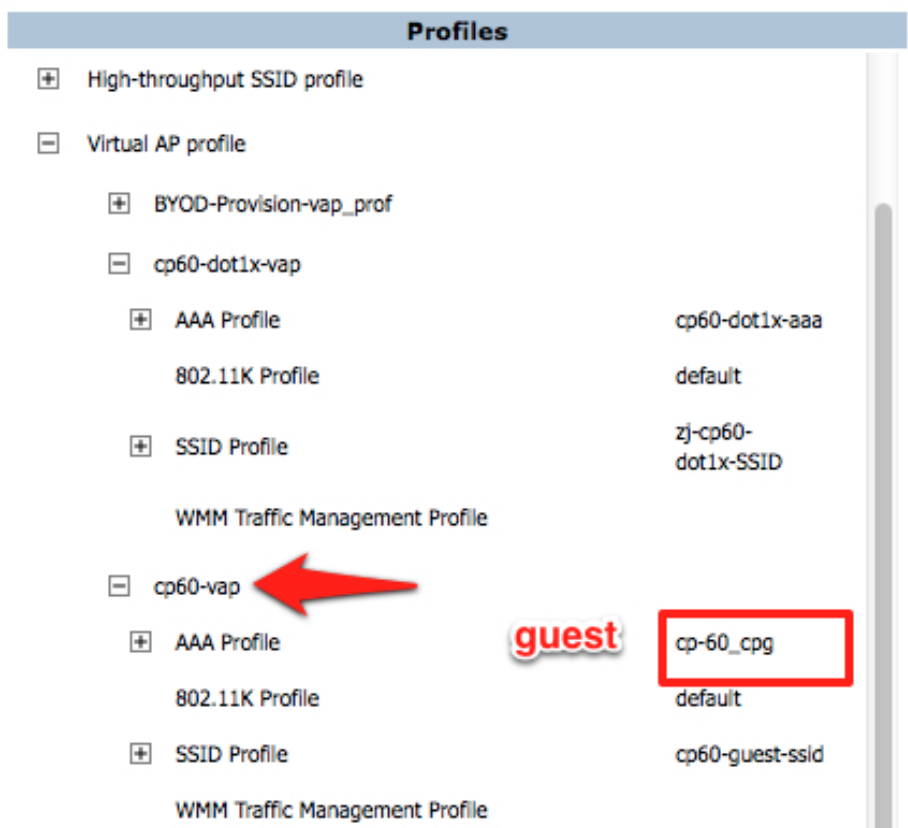
Figure 47 Advanced Services Virtual AP Profile

Advanced Services > All Profile Management



Modify each Virtual AP profile to use the appropriate AAA Profile that you created in the previous section.

Figure 48 Virtual AP Profile modifications



Make sure to click **Apply** after each change.

Click the **Save Configuration** button at the top of the page once the changes are completed.

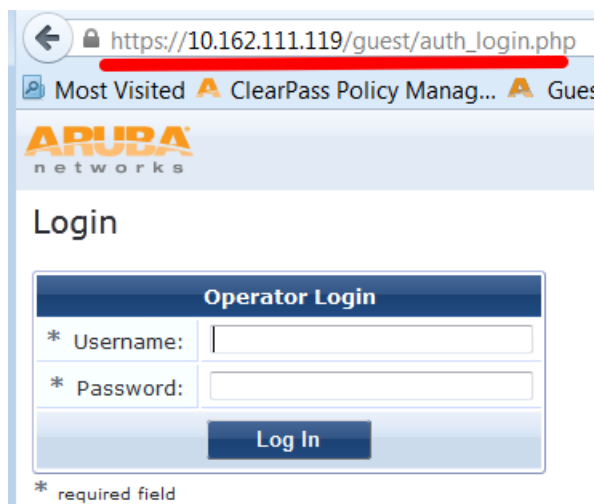
Step 8: ClearPass Guest Setup

In this step we will configure basic Guest Registration and Login.

Basic Guest Registration and Login configuration

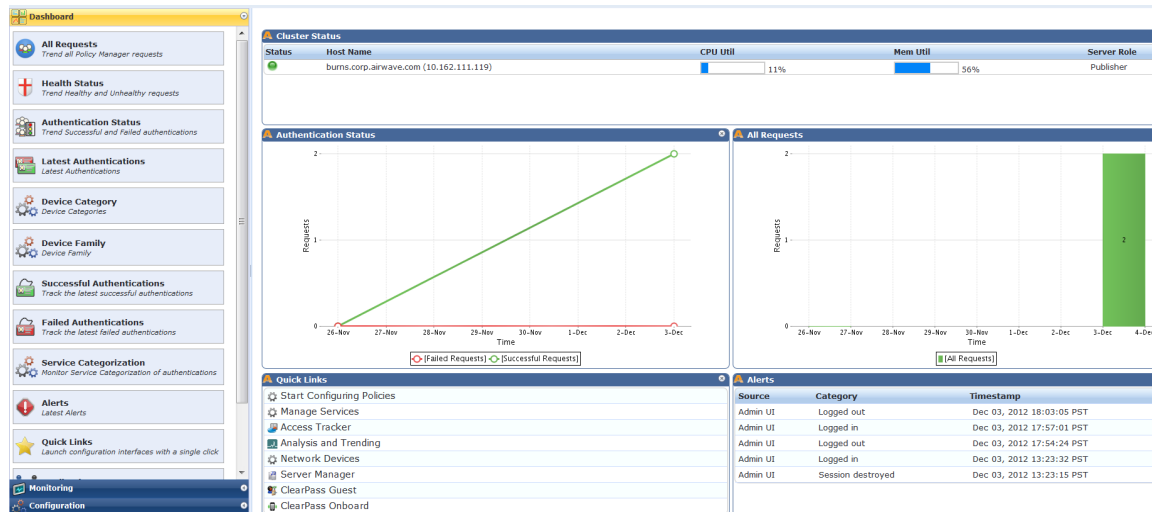
Log into ClearPass Policy Manager (<https://<your-cp-ip-here>/tips>).

Figure 49 Policy Manager login



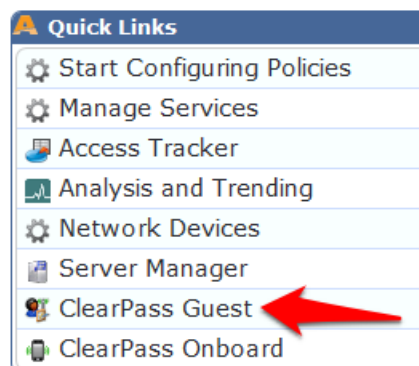
After you login, you will see the ClearPass Policy Manager Dashboard.

Figure 50 ClearPass Policy Manager Dashboard



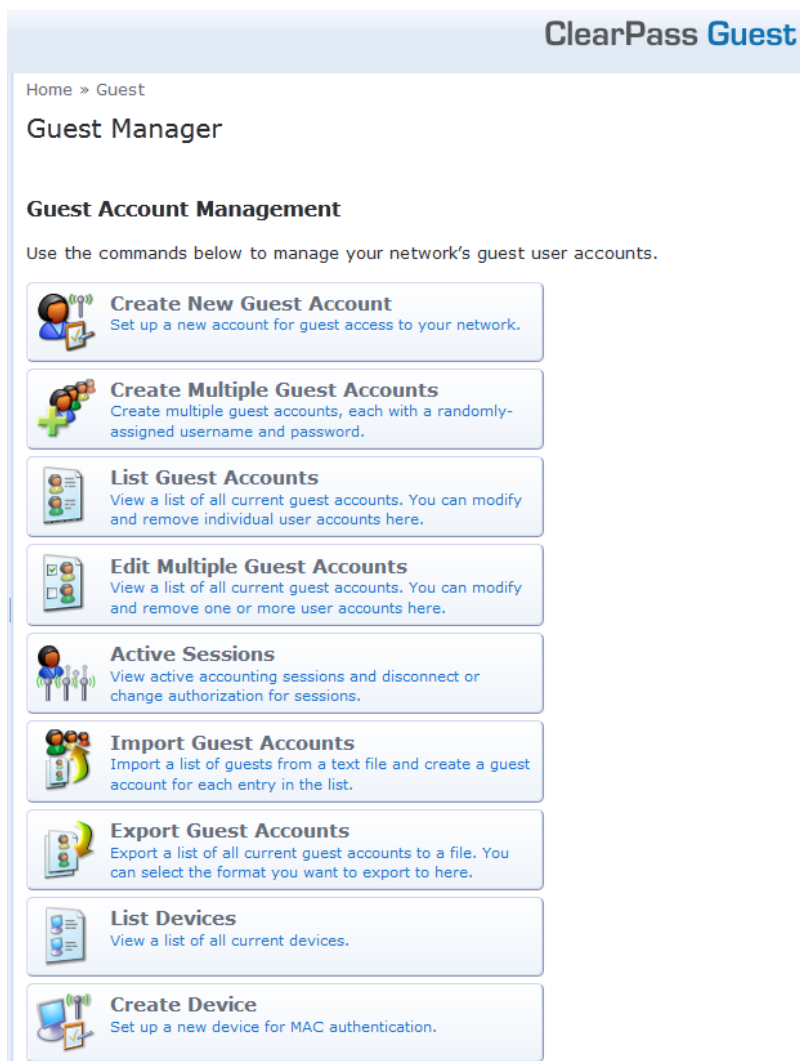
One of the Dashboard objects is Quick Links. Click on the quick link for ClearPass Guest

Figure 51 ClearPass Guest Quick Link



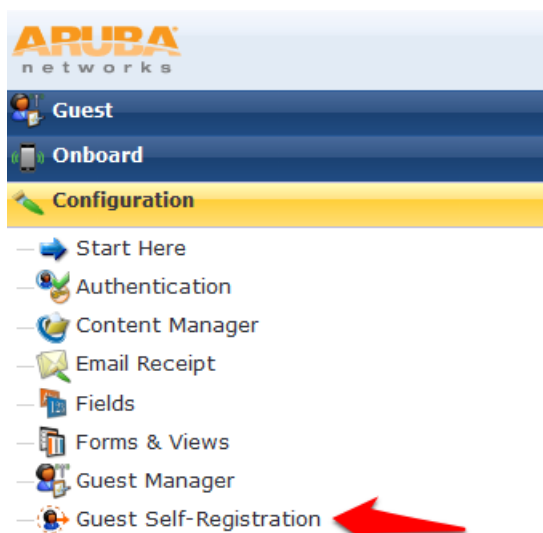
Clicking this link will automatically log you into the ClearPass Guest administration page. Alternatively you could enter the url for the Guest page) (<https://<your-cp-ip-here>/guest>).

Figure 52 ClearPass Guest administration page



Navigate to **Configuration->Guest Self-Registration**.

Figure 53 ClearPass Guest Self-Registration selection



Click on the preconfigured **Guest Self-Registration** profile. This will reveal several options. Click **Edit**.

Figure 54 ClearPass Guest Self-Registration menu

Home » Configuration » Guest Self-Registration

Guest Self-Registration

Use this list view to manage the pages used for guest self-registration.

Quick Help			
Name	Register Page	Skin	Parent
Guest Self-Registration Default settings for visitor self-registration.	guest_register	(Default)	(No Parent)
<a>Edit <a>Delete <a>Duplicate <a>Disable <a>Go To			
1 self-registration <a>Reload			
20 rows per page			

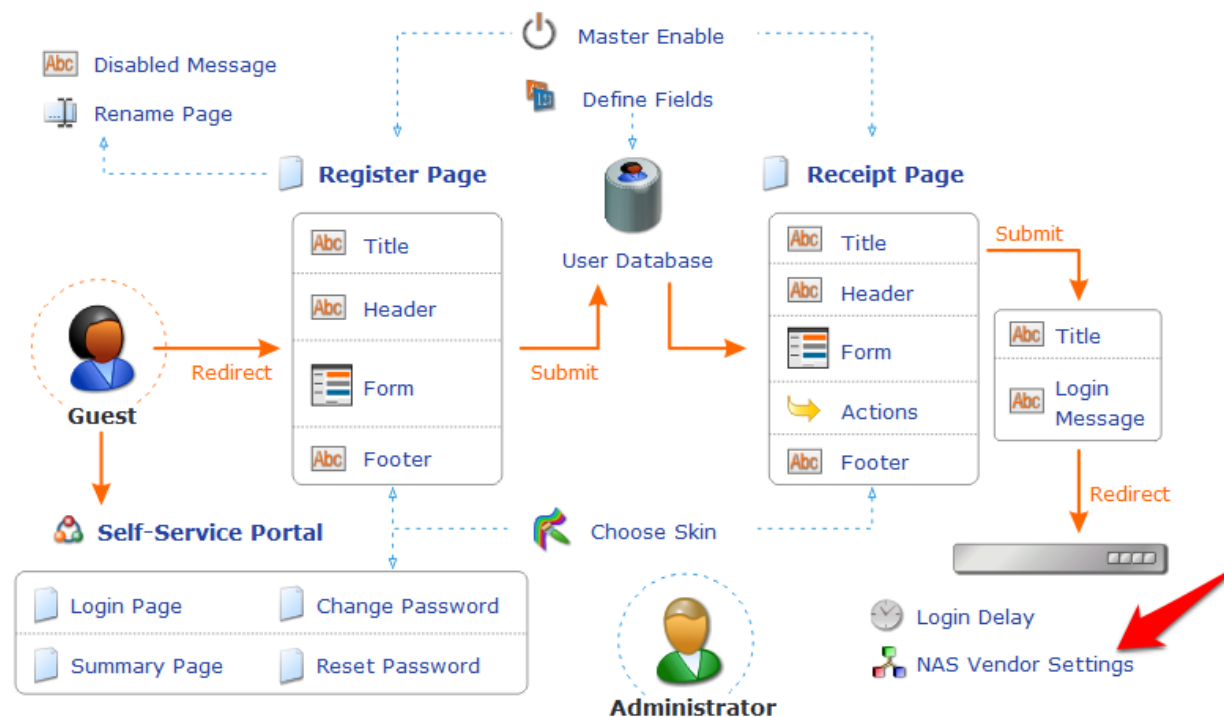
Back to configuration

Back to main

In this guest registration profile, it is necessary to enable web login. Click **NAS Vendor Settings** from the edit diagram:

Figure 55 NAS Vendor Settings

Guest Self-Registration 'Guest Self-Registration'



On the **NAS Login** settings page, check the checkbox to **Enable guest login to a Network Access Server**. It will prepopulate the settings with Aruba Networks NAS settings.

Figure 56 Enable guest login to a Network Access Server

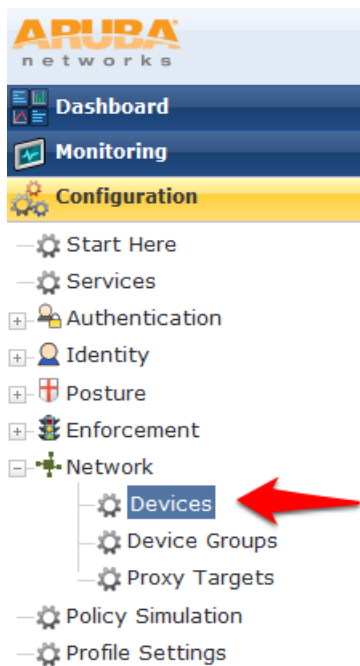
Customize Guest Registration	
NAS Login Options controlling logging into a NAS for self-registered guests.	
Enabled:	☒ Enable guest login to a Network Access Server
* Vendor:	Aruba Networks
Settings:	Select a predefined group of settings suitable for standard network configurations.
IP Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default Select a security option to apply to the web login process.
Dynamic Address:	☐ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Default Destination Options for controlling the destination clients will redirect to after login.	
Default URL:	 Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	☐ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
 Save Changes  Save and Continue	

Click **Save Changes**.

2. ClearPass Policy Manager Setup

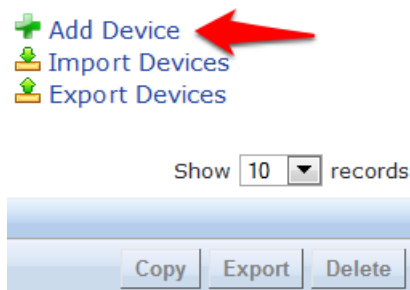
In ClearPass Policy Manager, navigate to **Configuration->Network->Devices**.

Figure 57 ClearPass Policy Manager Network Devices selection



Click **Add Device** in the top right corner of the page.

Figure 58 Add a ClearPass Policy Manager Network Device



Enter a **Name** and the **IP or Subnet address** for your Wireless Controller. For the RADIUS Shared Secret, enter <aruba123> (the same shared secret we used in the Controller setup for RADIUS and RFC 3576). Select **Aruba** as the **Vendor Name**, and check the box to **Enable RADIUS CoA**

Figure 59 Configuring a ClearPass Policy Manager Network Device

Add Device

Device | **SNMP Read Settings** | SNMP Write Settings | CLI Settings

Name: Aruba Test Controller

IP or Subnet Address: 10.1.1.10 (e.g., 192.168.1.10 or 192.168.1.1/24)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

Attributes

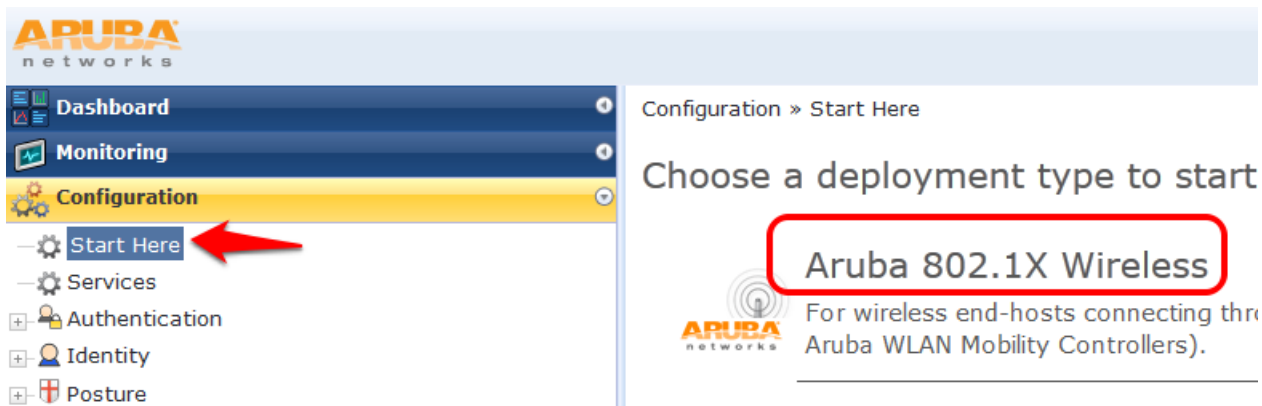
Attribute	Value
1. Click to add...	

Add Cancel

Click **Add**.

Navigate to **Configuration->Start Here** and select Aruba 802.1X Wireless.

Figure 60 Aruba 802.1X Wireless 'Start Here' selection



Give the service a name such as <WLAN Enterprise Service>.

Figure 61 Naming a 802.1X Wireless Service

Services



Service	Authentication	Roles	Enforcement	Summary
Type:	Aruba 802.1X Wireless			
Name:	WLAN Enterprise Service			
Description:	Aruba 802.1X Wireless Access Service			
Monitor Mode:	☐ Enable to monitor network access without enforcement			
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints			
Service Rule				
Matches ☐ ANY or ☒ ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		
4. Click to add...				

Click **Next**.

On the **Authentication** tab, Click the **Select to Add** down arrow and choose **[Local User Repository]** **[Local SQL DB]** as the **Authentication Sources**.

Figure 62 802.1X Authentication Methods and Sources

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:				
[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS]		Move Up Move Down Remove View Details Modify		
--Select to Add--				
Authentication Sources:				
[Local User Repository] [Local SQL DB]		Move Up Move Down Remove View Details Modify		
--Select to Add--				
Strip Username Rules:				
☐ Enable to specify a comma-separated list of rules to strip use				

Click **Next**.

For initial testing, **Role mapping Policy** will not be used. Click **Next** on the **Roles** tab at the bottom right corner of the page to continue.

Figure 63 802.1X Role Mapping Policy

Configuration » Services » Add

Services



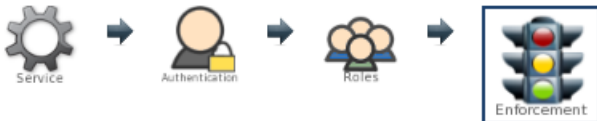
Service	Authentication	Roles	Enforcement	Summary
Role Mapping Policy: --Select--				
Role Mapping Policy Details				
Description:		-		
Default Role:		-		
Rules Evaluation Algorithm:		-		
Conditions				

On the **Enforcement** tab, no changes are necessary. Click **Next** at the bottom right corner of the page to continue.

Figure 64 802.1X Enforcement configuration

Configuration » Services » Add

Services



Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: ☐ Use cached Roles and Posture attributes				
Enforcement Policy: [Sample Allow Access Policy]				
Enforcement Policy Details				
Description:		Sample policy to allow network access		
Default Profile:		[Allow Access Profile]		
Rules Evaluation Algorithm:		evaluate-all		
Conditions				
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday,				

Review the summary and click **Save**.

Important! You must move the WLAN Enterprise Service above any generic RADIUS services that are not filtering via service rules. ClearPass 6.0.1 does not ship with any generic RADIUS services that have no service rules.

Navigate to **Configuration->Services** and select **Reorder** to move “WLAN Enterprise Service” above ANY generic RADIUS services that are not filtering via service rules.

Figure 65 ClearPass Policy Manager Reorder menu

ClearPass Policy Manager - Aruba Networks - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ClearPass Policy Mana... x Customize Guest Regis... x Guest Manager - Clear... x All Profile Management x W Table of keyboard shor... x +

https://10.162.111.119/tips/tipsContent.action#1354641429875

Most Visited ClearPass Policy Man... Guest Manager - Clear... Aruba controller interfa... Help Desk - Powered b...

ARUBA networks ClearPass Policy Manager Support Help Logout admin (Super Administrator)

Configuration » Services

Services

Services have been reordered successfully

Filter: Name contains Go Clear Filter Show 10 records

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	Guest Operator Logins	Application	Aruba Application Authentication	●
3.	3	WLAN Enterprise Service	RADIUS	Aruba 802.1X Wireless	●
4.	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
5.	5	Guest MAC Authentication	RADIUS	MAC Authentication	●
6.	6	Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	●
7.	7	Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
8.	8	Guest Access - Web Login Pre-Auth	RADIUS	RADIUS Enforcement (Generic)	●
9.	9	Onboard Authorization	RADIUS	RADIUS Enforcement (Generic)	●
10.	10	Onboard Provisioning - Aruba	RADIUS	Aruba 802.1X Wireless	●

Showing 1-10 of 11

Reorder Copy Export Delete

© Copyright 2012 Aruba Networks. All rights reserved. Dec 04, 2012 09:29:10 PST ClearPass Policy Manager 6.0.1.45884 on CP-SW-VA platform

Find: wireless Next Previous Highlight all Match case

Select <WLAN Enterprise Service> and click on the **Move up** button to position above ANY generic RADIUS services that are not filtering via service rules.

Note: Do NOT move any services you create ABOVE the initial services that are installed with ClearPass Policy Manager. **IF** you add a service and move it ABOVE the initial services installed your newly created service **could** intercept RADIUS requests that “Guest Mac authentication”, which is Mac caching, or Onboarding, and AirGroup.

Figure 66 Reorder Services 'Move Up' process

Configuration » Services » Reorder

Reorder Services

Order	Name
1	[Policy Manager Admin Network Login Service]
2	Guest Operator Logins
3	[AirGroup Authorization Service]
4	Guest MAC Authentication
5	Guest Access With MAC Caching
6	Guest Access
7	Guest Access - Web Login Pre-Auth
8	Onboard Authorization
9	Onboard Provisioning - Aruba
10	[Aruba Device Access Service]
11	WLAN Enterprise Service

Move Up Move Down

Service Details:
Name: WLAN Enterprise Service
Template: Aruba 802.1X Wireless
Type: RADIUS
Description: Aruba 802.1X Wireless Access Service
Status: Enabled
Service Rule
((Radius:IETF:NAS-Port-Type EQUALS Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Frame
AND (Radius:Aruba:Aruba-Essid-Name EXISTS))
AND (Connection:Protocol EQUALS RADIUS))

If you are running the beta version of 6.0, you may not have the Guest MAC Authentication services. If this is the case, please [download](#) the non-beta version of 6.0, as it will include these services by default.

Guest SSID Login service configuration

To configure the Guest SSID Login service, navigate to **Configuration->Services**. Click on **Guest Access With MAC Caching**.

Figure 67 Guest Access With MAC Caching

ARUBA networks ClearPass

Configuration » Services

Services

Filter: Name contains

#	Order	Name
1.	1	[Policy Manager Admin Network Login Service]
2.	2	Guest Operator Logins
3.	3	WLAN Enterprise Service
4.	4	[AirGroup Authorization Service]
5.	5	Guest MAC Authentication
6.	6	Guest Access With MAC Caching
7.	7	Guest Access

Click on the **Service** tab.

In order to get this service to respond to the guest SSID, click the **Radius:Aruba, Aruba-Essid-Name, EQUALS, <Guest SSID Name>** row under **Service Rule** sub-tab to modify.

Replace the <Guest SSID Name> with the actual guest SSID used on the controller.

In the example below, the guest SSID is: **zj-cpg60**

Figure 68 Service Rule Guest SSID conditions

Services - Guest Access With MAC Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name:	Guest Access With MAC Caching				
Description:	Service for guest access via captive portal (non-802.1x)				
Type:	RADIUS Enforcement (Generic)				
Status:	Enabled				
Monitor Mode:	☐ Enable to monitor network access without enforcement				
More Options:	☒ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints				
Service Rule					
Matches ☐ ANY or ☒ ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	Calling-Station-Id	EXISTS			
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}		
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	zj-cpg60		
4. Click to add...					

Click **Save** to register the modifications to the service.

Repeat those steps for the **Guest MAC Authentication** service:

Figure 69 Service Rule Guest MAC Authentication conditions

Services - Guest MAC Authentication

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name:	Guest MAC Authentication				
Description:	Service performing authentication for cached MAC entries for guest accounts				
Type:	MAC Authentication				
Status:	Enabled				
Monitor Mode:	☐ Enable to monitor network access without enforcement				
More Options:	☒ Authorization ☐ Audit End-hosts ☐ Profile Endpoints				
Service Rule					
Matches ☐ ANY or ☒ ALL of the following conditions:					
Type	Name	Operator	Value		
1. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
2. Radius:Aruba	Aruba-Essid-Name	EQUALS	zj-cpg60		
3. Click to add...					

The next step is to add a User Role. Even though no role mapping is in use in the WLAN Enterprise Service, a user role must be created for any local user account added into the Local User Repository.

Navigate to **Configuration->Identity->Roles**

Click **Add Role** in the top right corner of the page.

Figure 70 Adding a Local User Repository Device




Add Roles


Import Roles


Export Roles

Show records

Enter <TestRole> as the name, and click **Save**.

Figure 71 Adding a Identity Role

The screenshot shows the Aruba ClearPass configuration interface. The left sidebar contains a navigation tree with the following items: Dashboard, Monitoring, Configuration, Start Here, Services, Authentication (Methods, Sources), Identity (Local Users, Guest Users, Onboard Devices, Endpoints, Static Host Lists, Roles, Role Mappings). The 'Identity' and 'Roles' items are highlighted with red arrows. The main panel displays the 'Roles' configuration page. At the top, there is a breadcrumb trail: Configuration » Identity » Roles. Below this is a filter section with a dropdown menu set to 'Name' and a search box. The main content is a table of roles:

#	Name
1.	TestRole
2.	[TACACS Super Admin]
3.	[TACACS Receptionist]
4.	[TACACS Read-only Admin]
5.	[TACACS Network Admin]
6.	[TACACS Help Desk]
7.	[TACACS API Admin]
8.	[Other]
9.	[Onboard Windows]

Navigate to **Configuration->Identity->Local Users**. Click **Add User**. Enter the following information:

- User ID: <test>
- Name: <Test User>
- Password: <test123>
- Verify Password: <test123>
- Enable User: check box <(Check to enable local user)>
- Role: select <TestRole> from the drop down menu

Figure 72 Guest SSID Local User conditions

Add Local User ✕

User ID	test
Name	Test User
Password	••••••••••
Verify Password	••••••~•••••
Enable User	☒ (Check to enable local user)
Role	TestRole

Attributes

Attribute	Value	
1.	Click to add...	

Add **Cancel**

Click **Add**.

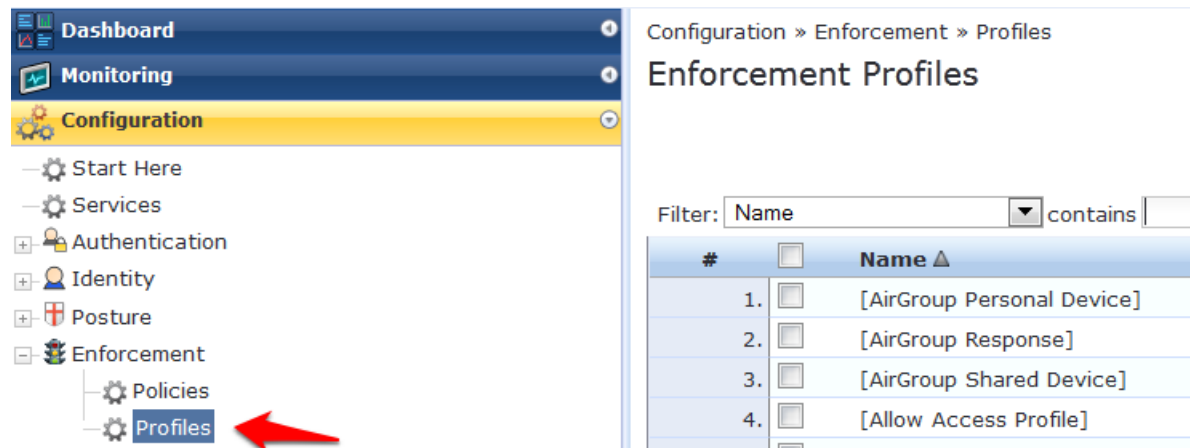
3. Testing the 802.1x and Guest SSID

At this point testing of the 802.1x and Guest SSID could commence. However, when 802.1x is tested with the Test User account, the user will authenticate but receive the guest role on the controller. This is because an Aruba User Role is not being passed back for the Test User. When the controller receives the RADIUS Accept from a successful authentication, the controller will give the client the default 802.1x role set in the AAA Profile.

In order to pass back an Aruba User Role, an Enforcement Profile must be built and the Sample Allow Access Policy must be modified to send this Enforcement Profile.

Navigate to **Configuration->Enforcement->Profiles**.

Figure 73 Configuring Enforcement Profiles



The screenshot displays the Aruba Configuration web interface. On the left, the 'Configuration' menu is expanded, and 'Profiles' is selected under the 'Enforcement' section, indicated by a red arrow. The main content area is titled 'Configuration » Enforcement » Profiles' and 'Enforcement Profiles'. It features a filter bar with 'Name' and 'contains' options. Below is a table listing four existing profiles:

#	Name
1.	[AirGroup Personal Device]
2.	[AirGroup Response]
3.	[AirGroup Shared Device]
4.	[Allow Access Profile]

Click Add Enforcement **Profile** in the top right corner of the page.

Give it a name like <Aruba Authenticated Role>. Make sure the **Template** selected is **Aruba RADIUS Enforcement**:

Figure 74 Adding a new Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Aruba Authenticated Role	
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- <button>Remove</button><button>View Details</button><button>Modify</button>	

Click **Next**.

Click on “**Enter role here**” and enter <authenticated> in the **Value** field as the role to be passed back. Then



click on the disk icon to save the line.

Click **Save**.

Figure 75 Enforcement Profile Attributes

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role (1)	= authenticated
2. Click to add...		

Click the disk icon to save the line!

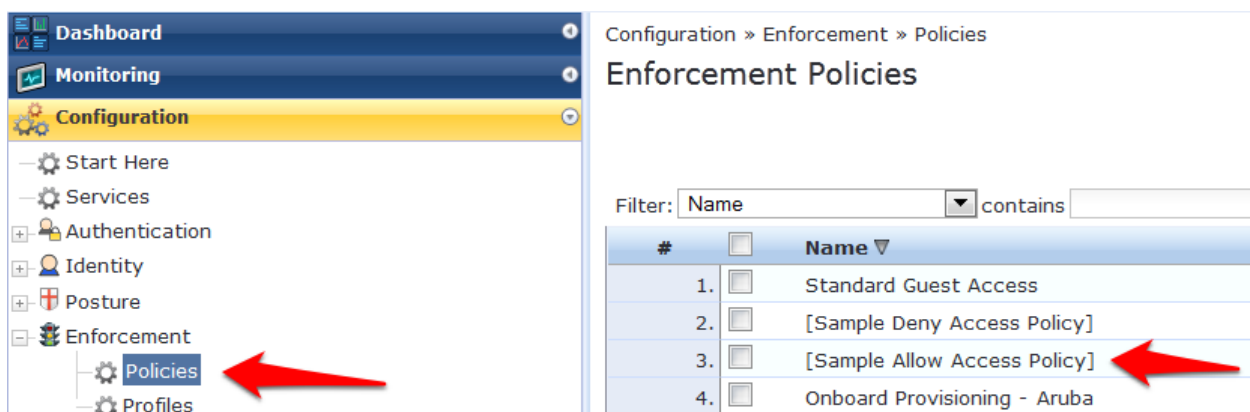
Tech Tip: Get used to clicking that disk icon. Whenever you edit a line like this, click the disk icon to save the line, or else your change may not get saved.

Click **Next**.

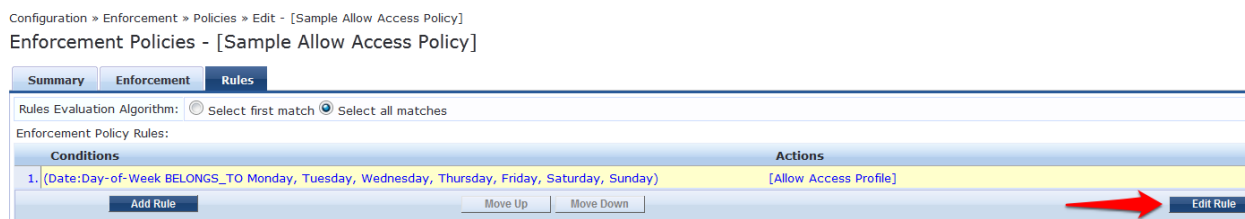
Click **Save**.

Navigate to **Configuration->Enforcement->Policies**. Click on the “Sample Allow Access Policy” to edit.

Figure 76 Enforcement Policies rule configuration

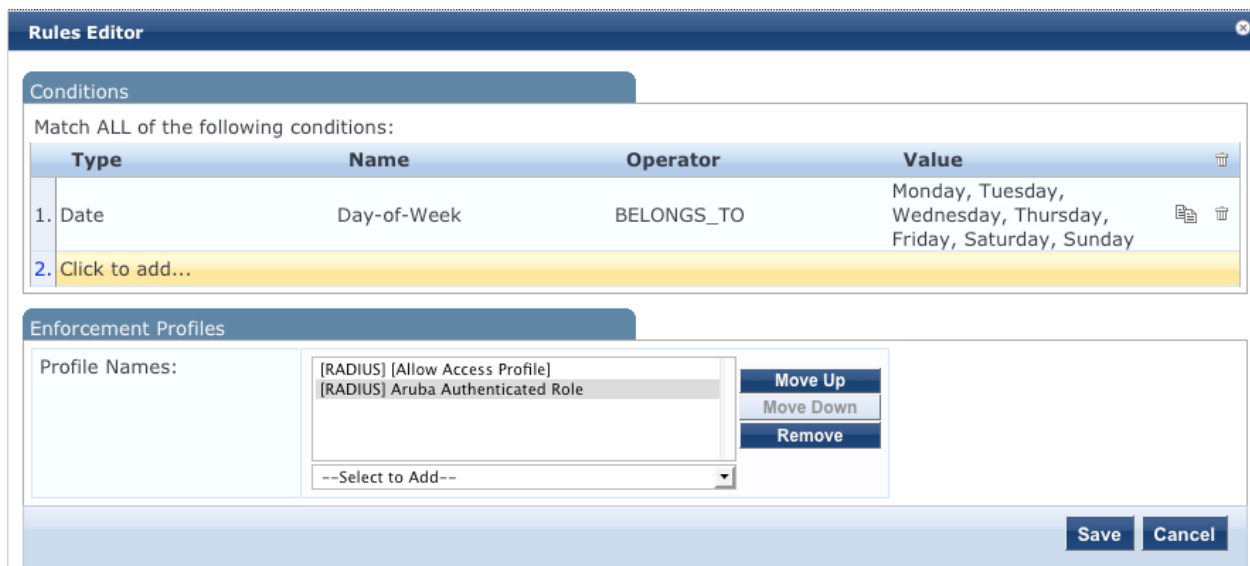


Click on the **Rules** tab. Click on the only Condition in the list to highlight it, and click **Edit Rule**.



Select the **Aruba Authenticated Profile** from the -- Select to Add -- drop down menu to the list of Enforcement Profiles that will be executed when a user successfully authenticates:

Figure 77 Enforcement Authenticated Profile Rules Editor



Click **Save** in the **Rules Editor** window.

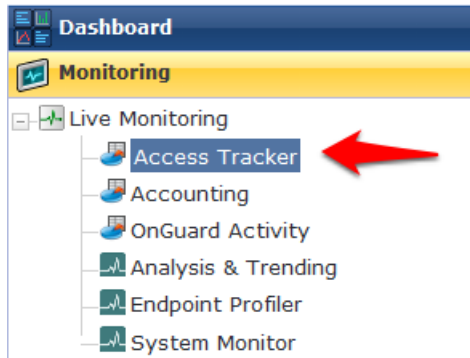
Click **Save** in the lower right corner of the page.

Step 9: Test the 802.1x SSID

Connect to the 802.1x SSID, and login with the local user account (NOT the guest account) created in the ClearPass Policy Manager setup.

Navigate to **Monitoring->Live Monitoring->Access Tracker**.

Figure 78 Live Monitoring Access Tracker menu



A **RADIUS, ACCEPT** for the WLAN Enterprise Service server should be visible.

Figure 79 802.1x SSID RADIUS, ACCEPT WLAN Enterprise Service

Access Tracker Nov 01, 2012 15:09:01 PDT Auto Refresh

Data Filter: [All Requests] Server: (10.1.1.20)
Date Range: Last 1 day before Today Edit

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	test	WLAN Enterprise Service	ACCEPT	2012/11/01 15:08:46

Step 10: Testing the Guest SSID

At this point, both the 802.1x SSID and the Guest SSID can be tested. Start by testing the Guest SSID.

In ClearPass Policy Manager navigate to **Monitoring->Live Monitoring->Access Tracker**.

When your device first connects to the Guest SSID you will notice a MAC Auth REJECT. This is for the MAC Caching on the Guest SSID.

Figure 80 MAC Auth REJECT for the MAC Caching on the Guest SSID

Access Tracker Nov 07, 2012 15:51:05 PST Auto Refresh

Data Filter: [All Requests] Server: (10.1.1.20)
Date Range: Last 1 day before Today Edit

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

Open up a web browser on your device that just connected. It should redirect you to the Guest Login page. Select **Click Here** after **Need an account?**

Figure 81 ClearPass Guest Login

Network Login

Please login to the network using your ClearPass username and password.

Network Login

* Username:

* Password:

* Terms:

☐ I accept the [terms of use](#)

✓ Log In

* required field

Need an account? [Click Here](#)

You will be then be presented with the Guest Account Creation page.

Figure 82 ClearPass Guest Registration

Guest Registration

Please complete the form below to gain access to the network.

Visitor Registration

* Your Name:

Please enter your full name.

* Email Address:

Please enter your email address. This will become your username to log into the network.

* Confirm:

☐ I accept the [terms of use](#)

✓ Register

* required field

Enter the information (Email Address will become the guest username), check the box to accept the terms of use, and click Register.

You will then be presented with the Guest Registration Receipt that shows the guest username and password.

Figure 83 ClearPass Guest Registration Receipt

Guest Registration Receipt

The details for your guest account are shown below.

Visitor Registration Receipt

Sponsor's Name:

admin

Visitor's Name:

Test User

Account Username:

 **test@test.com**

Visitor Password:

 **76435597**

Expiration Time:

Friday, 02 November 2012, 01:24 PM

✓ Log In

Clicking **Log In** button will automatically submit these credentials to the wireless controller's internal captive portal, which will create a RADIUS request with the Authentication Method PAP. This request will hit the Guest SSID Login Service that was created in ClearPass Policy Manager in the previous step.

After logging in on the test device, return to Access Tracker in ClearPass Policy Manager.

Notice the RADIUS ACCEPT entry for test@test.com:

Figure 84 RADIUS, ACCEPT configuration for a newly created 802.1x SSID Guest account

Filter: contains Show records

Server	Type	User	Service Name	Login	Date and Time ▾
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

STOP! Wait 3 minutes before proceeding to the next step. For MAC Caching, the service queries the Insight Database. Information is pushed to the Insight Database every 3 minutes.

4. Testing the MAC Caching

The next steps test the MAC Caching.

1. SSH to your controller and run:

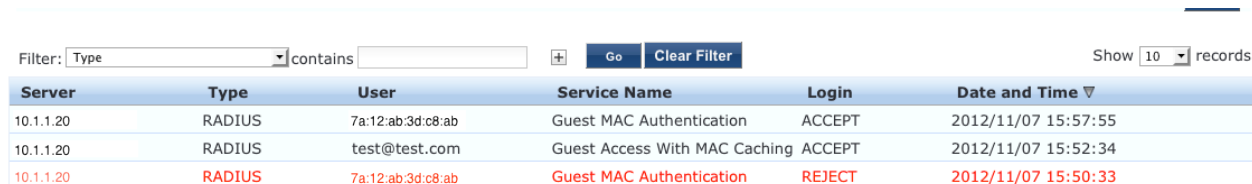
```
show user-table | include <test@test.com>
```


command where `<test@test.com>` is the 802.1x SSID guest user created, in order to find the MAC address of the test device.
2. Disable the wireless on the test device and run:

```
aaa user delete mac <00:aa:22:bb:44:cc>
```


command where `<00:aa:22:bb:44:cc>` is the MAC address returned from the `show user-table` command.
3. Re-enable the wireless on the test device. Now in Access Tracker you will see a successful MAC authentication.

Figure 85 Successful MAC authentication



Filter: Type contains + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time ▾
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	ACCEPT	2012/11/07 15:57:55
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

5. Advanced Features

Controller Management Login Authentication with ClearPass Policy Manager

In ClearPass Policy Manager, navigate to **Configuration->Identity->Roles**.

Click **Add Roles**.

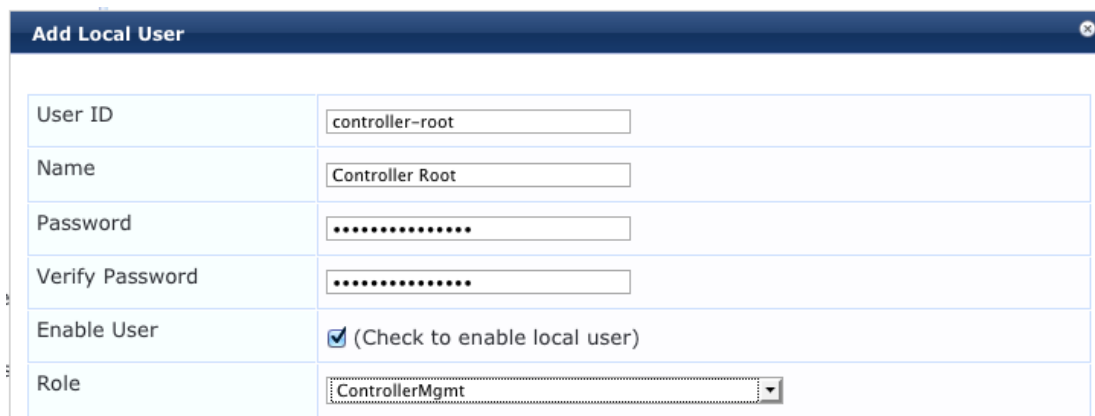
Create a new role called **ControllerMgmt**.

Navigate to **Configuration->Identity->Local Users**.

Click **Add User**.

Enter the information from Figure 86 Adding a Controller Management Local User, using whatever you want for the password (this will be the login and password for managing the controller).

Figure 86 Adding a Controller Management Local User



Add Local User	
User ID	controller-root
Name	Controller Root
Password	
Verify Password	
Enable User	☒ (Check to enable local user)
Role	ControllerMgmt

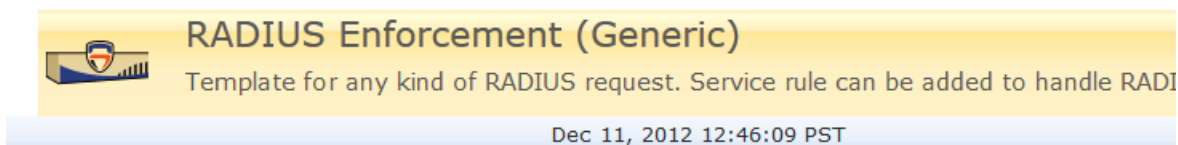
Click **Add** to save this user account.

RADIUS Enforcement (Generic) configuration

Navigate to **Configuration->Start Here**.

Scroll down the right main column and click on **RADIUS Enforcement (Generic)**.

Figure 87 RADIUS Enforcement (Generic) template



Service

Give the service a name such as <Aruba Controller Management Login>.

Add the Service Rules from Figure 88 RADIUS Enforcement (Generic) Service Rules configuration below for each Service Rule by selecting from each of their corresponding drop down arrow menu settings.

Figure 88 RADIUS Enforcement (Generic) Service Rules configuration

Service Rule				
Matches ☐ ANY or ☒ ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port	EQUALS	0	 
2. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	 
3. Radius:IETF	Service-Type	EQUALS	Administrative-User (6)	 
4. Click to add...				

Remember to click the disk  at the end of each Service Rule in order to save the line configuration.

Click **Next**.

Authentication

For **Authentication Methods**, Click the **Select to Add** drop down arrow and choose **[MACHAP]**.

For **Authentication Sources**, Click the **Select to Add** drop down arrow and choose **[Local User Repository]** **[Local SQL DB]**.

Figure 89 RADIUS Enforcement (Generic) Authentication configuration

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods: [MSCHAP]  Move Up Move Down Remove View Details Modify Add new Authentication Method --Select to Add--				
Authentication Sources: [Local User Repository] [Local SQL DB]  Move Up Move Down Remove View Details Modify Add new Authentication Source --Select to Add--				
Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				

Click **Next**.

Roles

Tech Tip: You could use a **Role Mapping Policy**, but it is not required. It would be required if the Authentication source was Active Directory, in which case you would create a Role Mapping rule that would look for the following configuration:

Authorization: SomeADServer:MemberOf:Contains:IT-Admins;

Role Name: ControllerMgmt

Click **Next**.

Enforcement

On the **Enforcement** tab, Click **Add new Enforcement Policy**.

Give the new Enforcement Policy a name like <Controller Login Enforcement>.

Figure 90 RADIUS Enforcement (Generic) Enforcement configuration

Enforcement	Rules	Summary
Name:	Controller Login Enforcement	
Description:		
Enforcement Type:	☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application	
Default Profile:	--Select to Add-- View Details Modify Add new Enforcement Profile	

Click **Add new Enforcement Profile**. Use the **Aruba RADIUS Enforcement** template. Enter a name for the Enforcement Profile such as <Aruba MGMT Root User>.

Figure 91 RADIUS Enforcement (Generic) Enforcement Profile Template and Name

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Aruba MGMT Root User	
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select--	

Click **Next**.

Add each Attribute from Figure 92 RADIUS Enforcement (Generic) Enforcement Attribute configuration below by selecting from each of their corresponding drop down arrow menu settings **except** for **Value**. Enter **root** in the **Value** field column.

Note: **Aruba-User-Role** is changed to **Aruba-Admin-Role**

Figure 92 RADIUS Enforcement (Generic) Enforcement Attribute configuration

Profile	Attributes	Summary
Type	Name	Value
1. Radius:Aruba	Aruba-Admin-Role (4)	= root
2. Click to add...		

Remember to click the disk



at the end of each Attribute in order to save the line

configuration.

Click **Next**.

Figure 93 RADIUS Enforcement (Generic) Enforcement configuration Summary

Profile	Attributes	Summary
Profile:		
Template:	Aruba RADIUS Enforcement	
Name:	Aruba MGMT Root User	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Aruba	Aruba-Admin-Role	= root

Click **Save**. This will return you to the Enforcement Policy creation.

Change the **Default Profile** to **Deny Access Profile**.

Enforcement	Rules	Summary
Name: Controller Login Enforcement		
Description: From the documentation procedure		
Enforcement Type: ☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application		
Default Profile: [Deny Access Profile] View Details Modify		

Click **Next**.

On the **Rules** tab, click **Add Rule**.

Enforcement	Rules	Summary		
Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches				
Enforcement Policy Rules:				
<table border="1"> <thead> <tr> <th>Conditions</th> </tr> </thead> <tbody> <tr> <td>Add Rule</td> </tr> </tbody> </table>			Conditions	Add Rule
Conditions				
Add Rule				

Enter the values from Figure 94 RADIUS Enforcement (Generic) Rule Conditions and Enforcement Profiles below for each Rules Editor Condition column by selecting their corresponding drop down arrow menu settings.

Figure 94 RADIUS Enforcement (Generic) Rule Conditions and Enforcement Profiles

The screenshot shows the 'Rules Editor' window. The 'Conditions' section has a header 'Match ALL of the following conditions:' and a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row contains 'Tips', 'Role', 'EQUALS', and 'ControllerMgmt'. The second row is a link 'Click to add...'. The 'Enforcement Profiles' section has a 'Profile Names:' label, a list box containing '[RADIUS] Aruba MGMT Root User', and buttons 'Move Up', 'Move Down', and 'Remove'. A red arrow points to the list box. At the bottom are 'Save' and 'Cancel' buttons.

Type	Name	Operator	Value
1. Tips	Role	EQUALS	ControllerMgmt
2. Click to add...			

Profile Names: [RADIUS] Aruba MGMT Root User

--Select to Add--

Save Cancel

Click **Save**.

Click **Next**.

Figure 95 RADIUS Enforcement (Generic) Enforcement Rules Profile Summary

The screenshot shows the 'Enforcement Rules Profile Summary' window with tabs 'Enforcement', 'Rules', and 'Summary'. The 'Enforcement' tab is active, showing fields for 'Name:', 'Description:', 'Enforcement Type:', and 'Default Profile:'. The 'Rules' tab is also visible, showing 'Rules Evaluation Algorithm:' and a table with 'Conditions' and 'Actions'.

Enforcement:

Name: Controller Login Enforcement

Description: From the documentation procedure

Enforcement Type: RADIUS

Default Profile: [Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role EQUALS ControllerMgmt)	[RADIUS] Aruba MGMT Root User

Click **Save** to log the Enforcement Policy.

The newly created Enforcement Policy should automatically be selected for the Service in the Service creation flow.

The screenshot shows the 'Service' configuration window with tabs 'Service', 'Authentication', 'Roles', 'Enforcement', and 'Summary'. The 'Enforcement' tab is active, showing 'Use Cached Results:' with a checkbox, 'Enforcement Policy:' with a dropdown menu set to 'Controller Login Enforcement', and buttons 'Modify' and 'Add new Enforcement Policy'. Below is the 'Enforcement Policy Details' section with fields for 'Description:', 'Default Profile:', and 'Rules Evaluation Algorithm:'. At the bottom is a table with 'Conditions' and 'Enforcement Profiles'.

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Controller Login Enforcement [Modify](#) [Add new Enforcement Policy](#)

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS ControllerMgmt)	Aruba MGMT Root User

Click **Next**.

Figure 96 RADIUS Enforcement (Generic) Enforcement Policy Service Creation Flow

Service	Authentication	Roles	Enforcement	Summary
Service:				
Type:	RADIUS Enforcement (Generic)			
Name:	Aruba Controller Management Login			
Description:	Aruba Wireless & ClearPass 6 Integration Guide example			
Monitor Mode:	Disabled			
More Options:	-			
Service Rule				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port	EQUALS	0	
2. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
3. Radius:IETF	Service-Type	EQUALS	Administrative-User (6)	
Authentication:				
Authentication Methods:	[MSCHAP]			
Authentication Sources:	[Local User Repository] [Local SQL DB]			
Strip Username Rules:	-			
Roles:				
Role Mapping Policy:	-			
Enforcement:				
Use Cached Results:	Disabled			
Enforcement Policy:	Controller Login Enforcement			

Click **Save**.

Note: Reorder the service so that it is **above** the **Guest Access With MAC Caching** service.

Reorder Services

Order	Name
1	[Policy Manager Admin Network Login Service]
2	Guest Operator Logins
3	[AirGroup Authorization Service]
4	Guest MAC Authentication
5	Aruba Controller Management Login
6	Guest Access With MAC Caching
7	Guest Access
8	Guest Access - Web Login Pre-Auth
9	Onboard Authorization
10	Onboard Provisioning - Aruba
11	[Aruba Device Access Service]
12	WLAN Enterprise Service

Move Up
Move Down

Click **Save**.

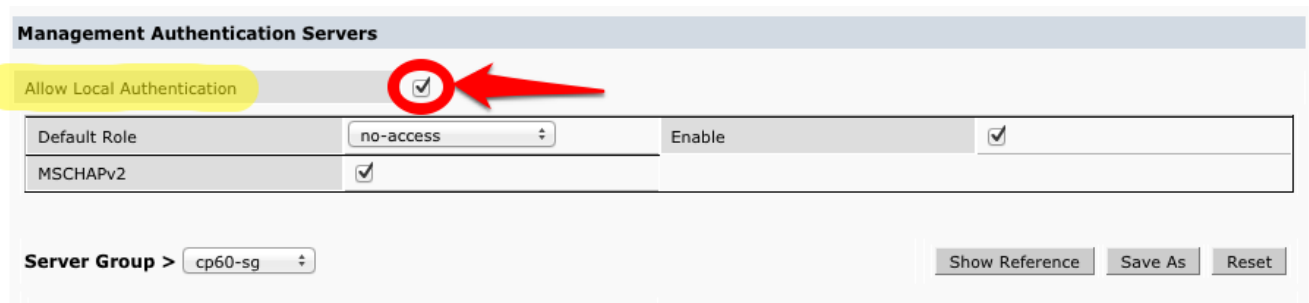
Management Authentication Servers

Login to the Aruba Controller Interface

Navigate to **Configuration->Management->Administration**.

1. Change **Default Role** to **no-access**.
2. Check the checkbox for **Enable**.

3. Check the checkbox for **MSCHAPv2**.
4. Change the **Server Group** to the ClearPass Policy Manager server group created earlier in this document.



Management Authentication Servers

Allow Local Authentication ☒

Default Role	no-access	Enable	☒
MSCHAPv2	☒		

Server Group > cp60-sg

Show Reference Save As Reset

Important! Leave the **Allow Local Authentication** box checked. If this box is unchecked and there is a problem with the Management Authentication configuration, you **will not** be able to login to the controller if **Allow Local Authentication** is unchecked.

Click **Apply** to save these settings.

Logout of the controller and test login with the controller-root test user created earlier.

In Access Tracker you should see the **Type = RADIUS** and **Login = ACCEPT** for the controller-root test user:

Filter: Type contains + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time ▾
10.1.1.20	RADIUS	controller-root	Aruba Controller Management Login	ACCEPT	2012/11/01 16:36:50

6. Troubleshooting

Problem:

MAC Caching is not working.

Solution:

Check the Endpoints Repository, navigate to **Configuration->Identity->Endpoints** for the device in question. Click on the device and verify that the device status is set to Known. If it is not, verify that the correct controller-ip vlan has been set on the wireless controller.

Problem:

During creation of Enforcement Policy, an error appears when trying to save: Name contains special characters...

Solution:

Creation of the Enforcement Policy has timed out. Click Cancel, then create the Enforcement Policy again.